OpenWrks

Consumer Data Right
Consultation on how best to facilitate participation of third party service providers

Consultation: Consultation on how best to facilitate participation of third party service providers
Deadline for Submission: 3 February 2020
Proposed CDR rules: Competition and Consumer (Consumer Data Right) Rules 2019

Completed by: Mitul Sudra, CTO & Co-Founder at OpenWrks
Contact: [redacted]

OpenWrks - Introduction & Background

At OpenWrks, we build the technology that makes Open Banking work. We've built the platform and applications that let people confidently view and share their account information with the businesses they trust so that everyone can get access to the financial products, services, and tools that they need the most.

OpenWrks have been supporting the UK's OBIE (Open Banking Implementation Entity) since 2017, and working closely with the CMA9 (the UK's 9 largest retail banks) and other stakeholders to define and develop the required APIs, security and messaging standards that underpin Open Banking.

OpenWrks were the first TPP (third party [service] provider) to be authorised by the FCA when OpenBanking was launched on the 13th January 2018 in the UK, and we were also the first TPP to successfully connect to all of the banks in the rollout of the UK's Open Banking framework. OpenWrks bring deep expertise, best practice and experience from our deep involvement in the UK Open Banking ecosystem - and keen to share this with the ACCC to increase adoption and make CDR a resounding success.

Today, we continue to provide both aggregation services and end user applications that power global fintech and financial services companies in providing secure, consent driven access to consumer and SME account and transactional data - at scale.

Specifically, we provide the underlying technology to allow UK's SMEs to securely share their banking data with Xero, and are executing a strategy to deliver the same service via CDR in Australia.

Links

- OpenWrks Blog
- Open Banking Profile

Press

- OpenWrks - first TPP (third party [service] provider) to be authorised by the FCA
- OpenWrks laying the API groundwork - https://www.cbronline.com/opinion/open-banking-apis
- OpenWrks "the first third party provider to successfully connect to all of the banks" - link
- Case Study: Collaboration between banks (TSB) and TPPs - link

Consultation

The ACCC has developed guiding questions for responses. You do not need to respond to each individual question and may decide to raise additional issues. Where possible, please explain your reasoning.

1. *If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that Consultation on the expansion of the Consumer Data Right rules 4 intermediaries can bring to the CDR regime and for consumers?*

    - OpenWrks intend to operate under two models; as an intermediary in the CDR regime (collect and use), and as a technology service provider (collect only) to intermediaries (commonly referred to as the TSP model in the UK). Under both models - we intend to provide:

        i. Aggregation services - providing a single API to access account and transactional data from all financial institutions and organisations under the CDR regime
        ii. Consent UX, a standardised UI/UX flow that manages user consent and bank/organistion selection, and banks redirection and return flows
        iii. A data transformation layer that regardless of the financial institution, provides normalised account and transactional data -
        iv. Enrichment services that further transforms normalised data and provides merchant and industry configurable categorisation of data
        v. Extended API capability that builds on CDR standards to help power richer experiences and more complex product use cases (at scale) - includes webhooks, transactional stitching, consent expiry management, downstream error handling.

        All of which provide a platform upon which products can be built on top of to power B2B and B2B2C propositions in the financial wellbeing, credit, debt management and broader financial services market.

2. How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.

    - OpenWrks encourages the adoption of both an outsourcing model and accreditation model. Our view is that the UK framework for how account providers (accredited intermediaries) and TSPs (outsource providers) can operate together strikes the right balance between governance of the ecosystem and accelerating new innovations and end user adoptions.

        For accredited parties we would expect similar levels of scrutiny before accreditation is awarded, including but not limited to assessment of the company's:

        - business plan
        - organisational structure
        - governance
        - monitoring and management of security incidents
        - monitoring and tracking sensitive data
        - business continuity

- information security management
- directors
- insurance and guarantees

For outsourced providers we broadly agree with the proposed decision to ensure appropriate arrangements are made between the accredited intermediaries and outsourced providers including the use of contracts to define the disclosure and recipient data flows/usage, deletion in accordance with CDR and the scope of these activities within the arrangement itself.

Beyond this list OpenWrks are of the opinion that outsourced providers should be required to demonstrate a subset of the accreditation requirements, possibly a standardised due diligence process which covers checks on the company and its directors, making sure the company and its directors don't appear on any sanctions lists, watchlists or enforcement registers.

In addition to this the review of information security and monitoring of security incidents and sensitive data is also recommended, which can be evidenced via globally recognised standards such as ISO27001:2013 which can provide an objective and impartial view of a company's information security maturity.

3. What obligations should apply to intermediaries? For example, you may wish to provide comment on:
    - if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards;

      See response to Q2.
    - if intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and intermediaries;

      See response to Q2.
    - if the obligations should differ depending on the nature of the service being provided by the intermediary.

      No, to reduce complexity for accreditation the same framework should be applied regardless of the service being delivered. The service being delivered should be reviewed as part of the intermediary's business plan to ensure consumer value is being delivered.

4. How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.

    - We advise reviewing the UK's Customer Experience Guidelines which covers the standards developed over the last 3 years including consent management/revocation, regulated party (accredited intermediary) transparency, data permissions, authentication flows, intermediary registry and ultimately how you put the customer in control of their data. We believe this model can be built upon and further improved to accelerate the CDR regime rather than starting from scratch.

5. How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of

redundant data, as well as any rules or data standards that should be met.

- The UK's Open Banking guidelines for management of consent, notification and deletion is built upon GDPR. The efforts by Australian parliament to update its privacy regulations to get closer to the EU framework is a positive move and should help underpin the rules for disclosure of CDR data between accredited persons.

  Similar regulations between the UK and Australia is a good outcome since standardisation makes the most sense and creates a common framework for citizens of all countries to use to manage their data.

  We recommend that any patterns and standards defined in the rules are underpinned by domestic legislation, but with a progressive view towards building innovative ways to secure and protect data and at the same time creating frictionless experiences for consumers and SMEs. This should include making the consent duration user defined rather than a fixed 90 day period.

6. Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?
   - See Q3
   - In addition we would recommend considering accreditation that relates to the activity being undertaken which creates tiers of accreditation. In the UK accreditation for Account Information Services (read only) and Payment Initiation Services (read and write) creates tiering linked to the level of risk to consumers (higher fraud/money laundering risk of write access for payments).

Consultation questions: permitting CDR data to be disclosed to non-accredited third parties

7. If the ACCC amends the rules to allow disclosure from accredited persons to nonaccredited third parties and you intend to: a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers; b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.
   - Please see goods and services outlined in Q1. Due to the broad capability and technologies we intend to deliver, we intend to operate under both models (depending on the service/customer we are providing). e.g.
     i. **receive CDR data as a non-accredited third party**
     We may work with a company like Xero where they act as the accredited person who discloses CDR data to non-accredited third parties. E.g. Xero outsource their connectivity to Australian financial institutions to OpenWrks to provide a technology solution. In this case we would be providing secure, API driven access for c.850k SMEs to manage their accounts and banking data through the Xero platform.

     ii. **be an accredited person who discloses CDR data to non-accredited third parties,**
     On accreditation of OpenWrks, we will be deploying our own applications and products into the Australian market which will involve the onward disclosure of CDR data to non-accredited third parties (B2B) which in turn allow consumers and SMEs to benefit from CDR. Our products (see https://www.openwrks.com/products):

1. **MyBudget - Income and Expenditure assessments re-imagined**
   Help your customers quickly and easily provide I&E using real-time verified transaction information, online, in minutes and at the touch of a button.
2. **Underwriters Dashboard - Get Open Banking insights with zero tech required**
   Enhance underwriting decisions, confirm repayment affordability or verify income with our underwriters dashboard. Quickly and easily get started with Open Banking data by adding our dashboard into your current processes.
3. **Money Coaching - Help your customers build a better financial future**
   Give your customers the support they need to save for today, tomorrow or for financial resilience. Money Coaching uses Open Banking and behavioural psychology to offer personalised challenges to reduce everyday spending.

In addition to this, OpenWrks would like to explore the feasibility of offering CDR data sharing capability for non accredited third parties that are building their own products and services where CDR data is only part of the product/solution/service. We work with several companies that effectively use our own AIS permissions (accredited status) under a regulated (via the FCA) *agency model*. The consumer is protected by it being transparent that OpenWrks is performing/providing the regulated activity (presentation of account information) as part of a wider application e.g. an app enabling aggregation of bank accounts to identify opportunities to reduce spending by switching provider.

8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?
   - Assuming the non-accredited third party demonstrates the maturity outlined in Q2, we do not recommend restricting the types of third parties to be able to receive CDR data. The liability and risk ultimately lies with the accredited party/intermediary and we feel this model is fair and works well in the UK (based on reported levels of fraud, breaches and data leakage). This is predicated on data ownership regulation which centres on the consumer (data subject) e.g. GDPR in the UK and EU. Under this consumer centric data regulation it is the consumers right to share their CDR data with a non-accredited third party and that third party's obligation to meet the data protection regulation to protect the consumer.

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?
   - Where a consumer chooses to exercise their right to share CDR data with a non-accredited third party, privacy and consumer protections should be provided through the Data Privacy Regulations or equivalent which any third party handling personal and private information has to comply with.

   - The UK framework does not stipulate that the consumer should be made aware of the non-accredited third party (in the TSP model). We agree with this approach as it simplifies the model for the consumer or SME in understanding the data sharing chain.

     e.g. The chain of end user (consumer/SME) > product/service (Xero cloud accounting) > bank (NAB) is already a complex mix of parties and introducing the disclosure of an outsource provider in the chain between the product/service and bank adds unnecessary complexity and confusion for the end user.

10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?
    - See Q4 - we propose a similar model detailed in the UK's CEG (customer experience guidelines). This includes consent UX/UI, presentation of accredited persons, permissions management and notifications to end users.
    - Ideally, where a consumer chooses to share CDR data with a non-accredited third party this can be captured by the accredited third party and made available to the consumer through a consent management service.