30 July 2021

Consumer Data Right
Commonwealth Treasury
Langton Crescent
PARKES ACT 2600

Lodged electronically: data@treasury.gov.au

Dear Sir/Madam

Consumer Data Right (CDR) Rules – Version 3

Origin Energy appreciates the opportunity to provide feedback on Treasury's Consumer Data Right (CDR) Rules amendments (version 3).

Unlocking the value of consumers' data is fundamental to promoting the benefits of a digital economy. However, when expanding the CDR regime, it is vital that the highest standards of information security measures are in place.

We are concerned that the proposed amendments lower the CDR regulatory standards for accreditation and increase the risk that consumer data will be transferred outside of the CDR ecosystem. Once CDR data leaves the ecosystem, CDR consumer protections will no longer apply. The success of the CDR regime is underpinned by consumer trust and industry reputation and the potential for consumer data to be stored or used in the manner that does not align with consumers' expectations must be avoided.

We believe there remains uncertainty regarding how the proposed changes will work in practice. This needs to be fully understood before this version of the Rules are finalised. Origin's response to each of the four main amendments to CDR framework set out in the Exposure Draft of the Rules - version 3 (the Exposure Draft) are set out below.

1. Sponsorship Model including CDR Representative and Outsourcing

Origin retains its support for a single tiered accreditation framework in the CDR regime. The current CDR Rules provide for one level of accreditation – this is at an 'unrestricted' level. This is considered the level of accreditation that ensures that Accredited Data Recipients (ADRs) have adequate system securities to request, hold and protect CDR data.

The Exposure Draft proposes three additional means in which a business could become accredited or act on behalf of the ADR[1]:

1. **Sponsored level of accreditation** will require a self-assessment and attestation as to establishment of information security capability. An 'unrestricted' ADR would then need to sponsor the business that they do meet the information security requirements;
2. **CDR representative model** removing the requirement to become accredited for participants that are subject to an arrangement with an unrestricted person that is liable for them; and
3. Collecting **outsourced service providers** (OSPs) enabling participants to rely on unaccredited third parties to collect CDR data.

We understand that the criteria for accreditation for both 'unrestricted' and the 'sponsor' model will be the same, however, an affiliate of its sponsor will not be required to provide an independent third-party assurance

[1] Exposure Draft Explanatory Material, Consumer Data Right Rules (version 3), p3.

report to establish that it meets the information security criterion once accredited. Instead, an affiliate (ie 'unrestricted' ADR) will be required to provide a self-assessment and attestation to the Data Recipient Accreditor (DRA) that the sponsored business meets the data security requirements.

The originating entities (ie banks, energy companies) are required to have the highest level of data security measures in place as they are entrusted in collecting and providing essential services to consumers. However, the sophistication of sponsored affiliates that will be handling CDR data and complying with the CDR Rules will vary. As a result, we are concerned that businesses that receive accreditation based on a 'contractual relationship' with an existing unrestricted ADR rather than having to meet the highest standards themselves will increase the risk of data breaches.

Information security requirements are critical to the effective operation of the CDR regime. Consumers want absolute assurance, that in providing consent to the release of their personal data, that it will be protected to the highest level. It is not sufficient for the penalty of non-compliance after the fact to sit with the sponsor, the Rules must have in place pre-emptive measures that will mitigate the risks of data breaches from sponsored affiliates.

While the Rules address the accreditation requirements, there are still some outstanding questions which include:

- Does the sponsored business take on liability and accountability (cover both accreditation and information security obligations) for any breach of the CDR Rules? If the sponsor is responsible to attest that the affiliate is complaint from an information security point of view, then they should take on accountability for breaches or non-compliance. It would be contradictory and provide little incentives for the affiliate to conduct a full diligence of a business prior to take them on if this was not part of the scheme.
- Will the 'sponsor' or 'unrestricted ADR authenticate with the customer?
- Will the customer know they are dealing with a sponsored company? Will the sponsored company be using the ADR branding?
- If a consumer has a complaint about data security, who does the consumer deal with - the sponsored ADR or the unrestricted ADR who attested to the business having the appropriate data security?
- Will sponsored ADRs have the same CDR obligations for deletion and destruction of data?

It should not be the intent of the CDR to create an incentive for smaller businesses to obtain the 'unrestricted' accreditation level and the bigger businesses to obtain the sponsorship level of accreditation. This could evolve to remove the requirement for a large business to obtain an independent third-party information security assurance report (which ADRs are saying are costly). That is, the smaller business may purely be the interface for the collection of data to comply with the Rules and the sponsored company performs the other CDR functions where the systems have not been independently verified as complying with the scheme.

The operational management of a sponsorship model must be worked through and be clear prior to any further consideration of this concept in the Rules.

In terms of the CDR representative and OSP models, the obligations between the 'unrestricted' ADR and the other parties acting on their behalf needs to be made clear. We have several examples in the energy sector where these types of models have led to ambiguity and increased reputational risk. For example, energy companies have used outsourcing models for door-to-door marketing for energy sales. Door-to-door marketing is now banned in the energy sector largely because businesses could not fully control the actions of all individuals of the third-party businesses that operated on their behalf. There needs to be clear obligations on any CDR representative or OSP models as to who is responsible for breaches and it needs to be clear to consumers who they are dealing with.

We support the continuation of a standardised accreditation process as is in the current CDR Rules. A single tiered arrangement will provide for data security and efficiencies for accredited data recipients that operate across sectors.

2. Transfer to Trusted Advisor

The Exposure Draft will allow a consumer to nominate a trusted advisor, including non-accredited persons such as an accountant, financial counsellors or lawyer to access CDR data. This is so the CDR consumer can receive professional services based on CDR data.

While this appears to be a reasonable function of the CDR regime, we are unclear how the ADR will confirm that the person the data is being directed to is actually a member of one of the classes of trusted advisors outlined in the Rules. It is assumed that there would need to be some verification through an industry identification or some other means to identify that the requested person is authorised to access the data.

This is a concern because once the data is transferred from an ADR to a trusted advisor, the CDR consumer protections will not apply as the data has been transferred out of the CDR eco-system. We accept the explanatory memorandum notes that Trusted Advisors are subject to their own existing professional or regulatory oversights (ie financial services licence) with regards to transfer of data, but consumers will not be protected if the data has been transferred to a person that is not appropriately registered as a member. For a consumer, there is little recourse for action if the data is misused.

For these reasons, traceability is critical to ensure that there are records of to whom and when data is transferred from an ADR to a Trusted Advisor. It seems logical that this would occur through the consumer dashboard.

We support further consultation on the technical standards prior to finalising this policy element of the Rules. Technical consultation is required on the use case scenarios by non-accredited persons to ensure consumers rights in relation to the identification, collection and use of CDR data are protected.

3. Disclosure of CDR insights

The Exposure Draft proposes to permit a CDR consumer to direct that particular CDR data be shared with Accredited Data Recipient's (ADRs) or Trusted Advisor's (as discussed above). The purposes for sharing the data as set out in the Rules is to: 1) identify the consumer; 2) verify the consumer's account balance; 3) verify the consumer's income; or 4) verify the consumer's expenses. While there is no proposed Rules that define 'verify', Treasury notes that it is intended to mean to confirm, deny or provide some simple information about the consumer's ID, business, account balance, income or expenditure based on their CDR data[2].

While we support the Rules providing a narrow purpose in which ADRs can request CDR insight data, there are still grey areas regarding: 1) how this will be interpreted by Data Standards Body (DSB) in the development of technical standards (particularly the extent to which they interpret the term 'verify'; 2) Rules that apply to the data once it is released to an ADR or Trusted Advisor (i.e. setting boundaries on the use); and 3) the extent to which a consumer understands the terminology for the release of data insights. The Exposure Draft does not appear to provide these boundaries, therefore increasing the risk of subjectivity in the interpretation of the Rules.

Any unintended use of data is most likely to impact vulnerable customers who may not know or understand that the consent to transfer data insights may have a negative impact on them accessing a good or service. For example, an ADR could request 'insight data' to determine the credit worthiness of the consumer and then use this information to determine whether the consumer can gain access to a particular product (ie energy or telecommunication plan). It may be questionable whether a CDR consumer, at the time of providing the consent, knew what the data would be used for. We support clear purposes in the Rules for the request of any insight data.

Should Treasury continue with the inclusion of CDR insights, to reduce the risk of this information being used in a detrimental way, the rules around how it is used once it is received by the ADR or Trusted Advisor ought to be tightened. This could include a requirement to explicitly explain the potential use of the data or limit the response to yes or no answers for all scenarios.

4. Joint Accounts

A fundamental consumer protection in energy is the concept of explicit informed consent. This means that a customer must actively provide consent before a retailer can make changes to their plan or whether information on their account is shared. We believe this principle must be preserved under CDR regime.

The Rules propose an amendment for joint account sharing settings to be set to 'pre-approval', allowing each joint account holder to automatically share data on the joint account. If one of the joint account holders does

[2] Exposure Draft Explanatory Material, Consumer Data Right Rules (version 3), p16.

not wish for the data to be shared, the account holder would need to actively provide notification to the data holder that they do not consent for the data to be shared – that is, change data sharing to 'off'.

We have several concerns with this proposal.

First, it is proposed that data will be provided in almost real time. If an account holder is required to 'opt out' of the data sharing, it is possible that the data will have already been shared by the time consent has been withdrawn. A customer may receive a notification, but then delay logging into the dashboard to remove consent. This would be an unacceptable outcome for a customer to have their information shared without their explicit consent.

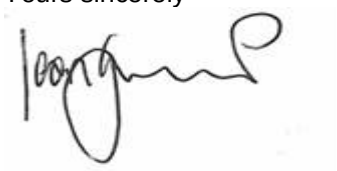
Second, when the consumer agrees terms and conditions with a data holder, the consent does not cover the use of data under CDR, nor does it contemplate that one account holder could request data through the CDR framework without the other account holder's consent. Energy companies hold a vast amount of consumer data and data subsets such as direct debts bank account details and consumer personal details (name, address, date of birth), which is highly sensitive data. Appropriate explicit consent should be provided by both account holders before this data is shared and there needs to be appropriate data security platforms for the receiving and transfer of such information.

We do not support a policy framework where the default position is that data is shared. If there is more than one account holder in a joint account arrangement, they should be required to consent for that data to be shared. 'Opt in' provisions ensure that consumers have control over their information and control over the future use of the data – this is specifically the case given the proposal for data to be shared outside the CDR ecosystem with trusted advisors.

It is noted that joint account provisions will only apply to the energy sector to the extent that our account set up process aligns with the joint account definition in the CDR Rules. While energy companies may not currently have accounts that meet this definition, it does not mean that these account establishment processes will not evolve in the future. We thus believe that CDR requirements should match industry regulatory frameworks.

If you have any questions regarding this submission, please contact Caroline Brumby in the first instance on (07) 3867 0863 or caroline.brumby@originenergy.com.au.

Yours sincerely



Sean Greenup
Group Manager Regulatory Policy