ADATREE
Your Consumer Data Right Partner

July 30, 2021

Adatree Response to Draft ACCC CDR Rules

Executive Summary

Adatree is pleased to provide commentary on the ACCC's draft changes to the CDR Rules. We appreciate that the ACCC and Federal Treasury have been collaborative with industry and listening to feedback. While it is a very difficult task to balance the consumer protections and high technical standards with decreasing barriers to entry for companies of all capabilities, this iteration of the Rules is a good first step towards this. This, however, falls short of meeting the actual goals of increasing access methods with meaningful change to enable the mission to enable a full range of customer value propositions.

The summary of key points:

- **Sponsor/Affiliate -** Other than the cost of audit, this model does not remove a single requirement for Affiliates compared to the current unrestricted ADR model. It essentially turns the sponsor into the role of an auditor or information security professional. Every single analysis of use case, compliance environment, CDR data boundary, policy, process, fit and proper framework and technical controls now lies with the Affiliate. This model will not result in meaningful increased participation in the CDR in its current form.
- **Insights -** This prescriptive allowlist of use cases is prohibitive to innovation and will inhibit future application insights. This needs to be aligned to the definition of 'sensitive information' in the *Privacy Act* to blocklist. This balances risks to consumers while increasing the breadth of insight based propositions.
- **Non-Accredited OSPs to Collect** must undergo a full ASAE3150 audit or equivalent, with clear requirements for information security controls, processes, policies, insurances and fit and proper. This is a risk to the companies that receive data downstream.
- **Trusted Advisers -** Mortgage brokers need to be considered for whom they can share information with, as there is a clear double standard for lenders that receive CDR data through a broker as opposed to directly from the consumer. Other professions, including insolvency practitioners and auditors, need to be added to the TA list.

About Adatree

Adatree has been a pioneer in the Consumer Data Right (CDR) since June 2019 with its turnkey Software as a Service platform for Data Recipients. Adatree's platform removes those complexities so companies can focus on leveraging data instead. Our platform enables companies across all industries to receive consented banking data via API in real-time.

Adatree takes the hardest part of the CDR, which is the technical and security standards and connections, and turns it into the easiest, with our platform accessed by one API. Adatree is also the only data recipient to provide business solutions to assist with accreditation.

Adatree is the first accredited and active CDR intermediary, and is one of five companies in Australia with Active ADR status in the CDR registry. Adatree is the smallest ADR yet received accreditation (including audit) in the fastest time. This shows our expertise in navigating the ecosystem and hands-on experiences with overcoming those challenges.

Our experiences are incredibly key to understanding the challenges faced by startups and smaller companies wanting to participate in the CDR instead of unregulated, unethical data sharing means (screen scraping).

Adatree recently signed Australia's largest ever bank/fintech partnership, with 24 ADIs selecting Adatree as their provider for CDR services that leverage Adatree's Industry Sandbox.

Sponsor / Affiliate Model

While this will be a popular model if implemented correctly, **this model does not make it easier for Affiliates to receive and leverage CDR data.**

There are two main barriers for companies wanting to be ADRs: the formal information security audit (e.g. SOC2, ASAE3150) and putting the policies, processes and technical controls in place.

While companies may say that the barrier is the external audit, it is actually the latter- the policies, process and technical controls. If a company had all of those in place, the audit would actually be a low and immaterial cost. The hard part is the policies, processes and technical controls. Adatree can hand-on-heart say this with our journey from creating all of these from scratch, identifying the fit for purpose controls and putting them in place ourselves, as well as working alongside our clients on their accreditation journeys.

What is required for a successful affiliate model is for the draft rules to specifically say what Schedule 2, Part 1 & 2 obligations are **not** required of the affiliate. The ACCC needs to strongly consider what aspects of the current unrestricted ADR application are not required. Removing the audit is not sufficient; it also does not acknowledge the value that third parties give to the accreditation readiness process. If the ACCC wants to make it easier for Affiliates to participate in the CDR, then they need to actually remove material tasks and obligations, not just shift the effort and cost to a third party.

Increasing burdens for sponsors: Sponsors are unreasonably left with the burden, role and responsibility of what is currently with the internal or external auditors and information security consultants. Treasury has not decreased the burdens for affiliates, other than an external stamp of approval. The analysis that the auditor and the ACCC Accreditation team had completed from a technical and compliance view for unrestricted ADRs has now shifted to the sponsor. Expecting the burden of advice for documentation, training, advice, use case analysis, and everything required for an ADR to be shifted to the sponsor is totally unreasonable. Again, this doesn't make life easier for any participant.

Suitability is subjective: CDR deals with 'fit for proper' persons, and in the draft rules (Schedule 1, 2.2(1)(a))), it says that the sponsor must ensure they are suitable. Suitable is not measurable and is only subject to interpretation. This does not make sense in a regime where everything is prescriptive and things are rarely interpretive. There needs to be guidelines or requirements in place for suitability.

Leave it to the professionals: The wording says a sponsor would have to provide "assistance or training in technical and compliance matters" to the affiliate. While sponsors are knowledgeable about technical and compliance matters, sponsors surely are not experts or consultants in this matter. Considering the sponsors would have to provide assistance, this leaves actual infosec professionals out of the equation. Sponsors would be forced to turn into infosec consulting businesses, if we have to give advice instead of relying on third party professional auditors or consultants.

Wording needs to be incredibly clear about what sponsors must do and not do, and who else can provide these services. The current blanket wording puts too much onus on the sponsor and leaves other participants out of the ecosystem.

Adatree currently discusses our own experiences relating to accreditation,, but providing affiliates advice en masse for their own use cases, technical compliance, controls and training shifts the responsibility unnecessarily to the sponsors. Liability needs to be incredibly clear for all parties. What if the sponsor gives advice to the affiliate for processes, controls or documentation and the affiliate doesn't do it, resulting in a breach or complaint?

The role of a third party auditor is incredibly important in this. While Adatree has the fastest ASAE3150 in the CDR ecosystem, we surely did not do everything on our own and have received much structure and guidance from professionals. One of the hardest and longest parts of the accreditation process is understanding the CDR environment, use case and application to rules, and applying the controls to the environment and ensuring it is properly documented. **The draft sponsor/affiliate rules do not remove any of this work that an affiliate does.**

Non-sensible timing: The timing of having an Affiliate accreditation subsequently getting a sponsor arrangement within three months should change. The arrangement needs to be in place *before* the affiliate accreditation is granted. The affiliate would have the 'PR spin' of being accredited and with no access to data or any hint of technical controls or a CDR

compliant environment. Most importantly, there is also no time for the technical or compliance advice mentioned above. This is also important should an affiliate change sponsors.

Self-Attestation & Self-Assessment: The Affiliate should complete and provide the self-assessment and self-attestation directly to the ACCC, and a Sponsor should be able to be notified of the assessment taking place and that the ACCC has accepted it. This would essentially serve as a new ACCC self-assessment affiliate register. Ultimately if an affiliate is in breach, this relationship would sit between the ACCC and affiliate, not the sponsor, therefore the ACCC should manage this self-attestation official process. It would also give more weight to the self-attestation/assessments in regards to the truthfulness of the statements should it ever go to the ACCC Compliance and Enforcement teams.

Principal / CDR Representative

With the CDR Representative, should a Principal collect on a Representative's behalf, we believe that it is too far removed from the rules, standards and requirements for an ADR in regards to policies, processes and information security controls for CDR data storage. It should be required that if a principal has a CDR representative, a data enclave is used. The ACCC could provide an example onboarding guide of what is required for a CDR representative, even with must haves, should haves, or optional aspects. It is unclear if a CDR representative needs to have technical controls, frameworks, policies and processes in place, and this needs to be clarified.

Adatree believes the data enclave could support the CDR representative model with data being stored in the CDR environment of the principal. This would ensure that the CDR data has all required controls, environments and audits in place while still enabling other companies.

Non-Accredited OSP (NAOSP) to Collect

Adatree itself was accredited for the purposes of collection of CDR data to enable others. As the ACCC and Treasury know, our own investment with time, money and effort into the pre-go-live testing and further advancement of the CDR ecosystem has been incredibly immense and critical to the ecosystem.

After Adatree's own journey to accreditation and active status, we believe that all companies that collect need to be at least fully audited. They would still need to ensure fitness and proprietary for persons accessing CDR environments, as well as requiring insurances and the full ability to support Schedule 2, Parts 1 and 2 information security controls. . This leaves no carrot for companies to collect and do the right thing by the CDR and consumer if others can operate at a lower cost while being a pivotal part of the CDR ecosystem while disregarding regulatory requirements and introducing risks to the ecosystem.

This introduces risks of the whole CDR downstream of companies accessing and relying on that data collected through companies without formal assurances. Companies collecting CDR will have a huge chain of companies accessing, leveraging, and sharing data, and creating insights. If the company at the beginning of the data collection process doesn't uphold the technical and security requirements, this is a risk to the CDR ecosystem and the very consumers leveraging those services.

For this access model, there should still be very clear requirements introduced relating to:

- The audit scope and requirements for the NAOSP
- What the NAOSP can and cannot do with the CDR data (e.g. in regards to collection, storage, analysis, etc)
- Associated privileges, CDR logos, and access to the CTS and CTS ServiceNow
- Whether the NAOSP would be considered Active on the register
- CTS requirements and liabilities for breaches of standards and rules for the NAOSP
- Complaint and dispute obligations

Insights

The addition of insights are welcomed but severely limit any type of innovation with the specified use cases. There is an incredible amount of low risk insights that are not listed. The list is finite and is the tip of the iceberg for insights.

The list of permitted insights need to be **principle based, not prescriptive; inclusive, not exclusive.** The current proposed list is severely limited.

What is missing is any type of creativity reflecting in the insight list. For example, here are **low-risk insight examples** that wouldn't be permitted within these rules due to lack of out of the box thinking.

1. Analysing whether a customer has used BNPL in the past month (yes/no)
2. Verifying an account type (confirmation of fact)
3. Whether a customer has bought a certain category of food (yes/no)
4. Whether a customer has bought a certain category of drink (yes/no)
5. Verifying an account status (closed / active) to process an authorised debit (yes/no)
6. Confirmation whether a transfer been made (confirmation of a fact)
7. Insight whether there are fees charged to the account (yes/no)
8. Whether a customer has surpassed their PlayStation Store spending limits (yes/no)
9. Whether a customer is eligible for a discount (yes/no)
10. Whether a customer is likely to have an investment property (yes/no)
11. Whether a business is eligible for government grants

The draft rules say 'verifying', and this wording itself is restrictive. An analysis should be included. It should also include **confirmation of a fact.**

The explanation in the EM also differs from the rules, where the former says 'a balance at a point in time' and this isn't reflected in the rules. Please address this discrepancy.

The more suitable definition of an insight is to **blocklist instead of allowlist**. The insights blocklist should align with the definition of *sensitive information* in the *Privacy Act (1988)*. If an insight does not fall into that blocklist, it should be allowed. It is not up to the ACCC to determine which customer value propositions based on insights should be allowed. Assuming that non-listed insights are not low risk is incorrect. The ACCC should be involved with compliance and enforcement of high risk insights, and shouldn't be the gatekeeper on what an appropriate insight is or isn't.

These examples above are purposely a mix of non-financial services. This current list is not acceptable and limits the consumers ability to access insight-driven services. Realistically, the most interesting ones haven't been thought of yet, and the rules need to enable, not stifle, innovation economy wide.

SCORES NEED TO BE INCLUDED

One key **insight that is missing** is a score.

Scores are often thought of as relating to credit, but a score could be calculated for a consumer that may be eligible for a discount based on certain eligibility. The discount would change based on a customer score of 1-10. If the consumer shares their CDR data, is analysed and the insight is say an 8, this could be sent to the retailer to apply a discount. Right now this use case is not allowed despite it being incredibly low risk, beneficial to customers, innovative and at the core of the CDR ethos.

In the same vein that trusted advisers (may) be able to access CDR data since they're trusted and already receive the data, a score is not any more dangerous to a consumer than any other insight. Scoring of applicants and customers is already commonplace practice, and not including scores would encourage non-CDR data collection means.

If insights scopes are not drastically increased, this leaves no incentives for companies to participate in and leverage CDR and use controversial alternative methods (e.g. screen scraping) to reach their goals. This would harm consumers with sharing their passwords with no controls and parties selling their aggregated data, instead of giving consumers the control and choice to make their own informed decisions.

INSIGHTS NEED SAME APPLICATION FOR ACCREDITED & NON-ACCREDITED PARTIES

Insights are discussed so that they can be disclosed to non-accredited parties and considered non-CDR data held and actioned outside of a CDR data environment. This suits non-accredited parties but this is not suitable for accredited parties. **This needs to change so an insight is considered non-CDR data to both accredited and non-accredited parties.**

If Adatree, an accredited and active ADR, wants to receive data for the purpose of account verification, then initiate a payment, the systems to debit an account are still in scope for the CDR data environment since the 'insight' of the account verification is still considered CDR data.

If the insight is passed onto a non-accredited party, they can store it in their non-CDR environment and action the payment, without that being in scope of an audited CDR environment. They are free and able to initiate other actions based on this insight, but accredited parties do not have the same freedoms.

This rule makes it easier for non-accredited persons to innovate with CDR insights, but immediately stifles the innovation of an accredited person. This is unacceptable and is an overlooked double standard.

Trusted Advisers

Adatree in general supports this. The draft rules should, however, provide guidance if not rules for how trusted advisors store CDR data. Right now this is a free-for-all of once it hits the Trusted Advisor, all technical controls are history. This could be stored on a portable USB held by a BAS agent. Treasury could consider attestations about storage and deletion for trusted advisors at the very least; more increased measures could include more prescriptive storage options. One option for this is that trusted advisers could store data in a data enclave provided by an ADR.

It is understood that trusted advisers access consumer or business financial data now, but increasing their technical security standards wouldn't be a bad upgrade for consumer protections, as long as reasonable and not heavy handed.

It should also be clear if trusted advisers are also able to de-identify the data or if deletion is the only end of consent option.

It is very unclear about how the trusted advisors would work in regards to mortgage brokers. Realistically, a consumer would consent to share their CDR data with a mortgage broker, which works via an ADR to give the CDR data to the broker. This works with the rules, but the journey with a mortgage broker never ends here. All other professions listed have consumer data shared with them to provide a service, from A to B. Mortgage brokers are different since data is only shared with them for the specific purpose of giving that data to a lender.

The clear loophole is that a lender has double standards in two scenarios. If they receive CDR data through a mortgage broker, they don't have to be accredited, reciprocity doesn't apply, and there's no customer consent or deletion. If they receive CDR data directly from a consumer, they have to be accredited (or an affiliate/representative) with actual barriers to entry. There is no incentive to receive data directly, and funnelling through a broker has dramatically different standards and requirements, without the same consumer protections. Shouldn't a consumer be able to consent that the broker shares with a certain bank and deletes their data accordingly if they want?

Insolvency practitioners and auditors need to be added to the TA list.

General Gaps

We would suggest creating clear diagrams of the relationships with the different models of what is and is not permitted. There will realistically be a long chain of companies helping bring CDR services to life. The different permutations of what is and is not permitted is necessary for what entities can and cannot work with others and/or provide services. It has gone from just an unrestricted (and active) ADR to consumer, to now having a maze of possibilities. How can Treasury ensure that there will still be high availability and ensure consumer data protections with so many companies in the chain of data sharing?

For the most inclusive example, there could be a non-accredited OSP collecting (which Adatree does not support), which is the data collection method for an unrestricted ADR, which is a sponsor for affiliates while also having CDR representatives, who offer insights to non-accredited persons. This doesn't even include OSPs.

Adatree strongly suggests delineating with responsibilities and defined terms for companies that are **active** versus **accredited**. For the sponsor/affiliate model, the sponsor can only be an active sponsor, not an accredited sponsor. The same goes for CDR representative, trusted advisors and insights.

Something missing is a prescriptive list of what an OSP is required to have, the same way that there's a lot of prescriptive material on how to be an ADR and meeting those requirements.

Ideally a chart showing the differences between all different access models or entity types would be helpful.

Clear Logo Differences: Companies with affiliate accreditation (or any other class that isn't unrestricted) should not be able to use the same CDR logo as unaccredited ADRs. They should have a separate class of logo so someone can distinguish the classes of ADRs.