SISS Data Services submission to Treasury in response to proposed Consumer Data Right rules amendments (version 3).

August, 2021.

INDEX

1. Summary

Sr. No	Subject matter for consultation and relevant provision under Rules	Issue	Proposed Resolution
1.	Trusted Adviser – (Rule 1.10C and Explanatory Notes)	Lack of detail in the due diligence process for vetting Trusted Advisers.	Treasury should provide details of the reasonable steps which ADRs should adopt for verifying Trusted Adviser.
		Frequency of verifying Trusted Advisers against their professional body/membership, to reduce the risk of CDR data being shared with a Trusted Adviser that is not part of a professional body.	Ensure that a Trusted Adviser register is updated for verified and eligible members no less than daily.
		Maintenance of Trusted Adviser internal register.	In order to ensure appropriate verification of Trusted Advisers, Treasury maintains or provides for a system through which ADRs can verify the professional membership of Trusted Advisers. Additionally, ADRs could be required to maintain and update their own Trusted Adviser register.
		Portability for vetting Trusted Adviser.	Allow ADRs which fulfil an eligibility criteria to provide vetting of Trusted Advisers as a separate service line.
2.	Sponsorship Accreditation (Rule 1.10D)	Accreditation for Addons are not portable.	A system/provision which allows add-ons of an affiliate to enter the CDR regime and access CDR data through the sponsorship model.
		ADRs responsibility to provide training to affiliates.	Clarity is sought on several aspects relating to providing training to affiliate. For instance, if sponsor can outsource such responsibility to third party, period/ frequency in which such training is provided, what should be the content and material topics for training, what evidence are required to be maintained by ADR towards providing training.
		Format and requirement of Self-assessment process.	The specific format of self-assessment and items which should form a mandatory part of self-assessment criteria, which cannot be compromised by the affiliate.
3.	CDR Representative (Rule 1.10)	Regulatory oversight required as not to encourage risk taking, thus undermining the CDR.	Allowing unaccredited Outsourced Service Providers (OSPs) to collect CDR data is a race to bottom, and the risk involved in allowing unaccredited data collectors to enter the CDR regime is much greater than the reward. The ACCC need to provide regulatory oversight of ADR offering a CDR representative model to ensure they have capability, resources to manage a CDR representative

2. About SISS Data Services

SISS Data Services (SDS) is an Accredited Data Recipient (ADR) and has been providing secure bank data solutions as an Intermediary to Fintechs for over ten years. All SISS bank data services operate with the consent of both the banks and the account holders. SISS does not use screen-scraping. Based on our extensive experience, we strongly believe in securely transferring only specific consumer-consented data to the specified SISS partner.

Intermediaries such as SISS Data Services, operate under agreements with Data Holders and maintain appropriate systems and processes to ensure consumer data is protected. Access to Consumer data is provided directly by the Data Holder under data supply agreements that adhere to the provisions of relevant regulations, including the Privacy Act. Data Holders only grant data access once the intermediary has demonstrated that they:

- have a robust consumer consent process (not screen scraping) which only allows access to specified accounts.
- have appropriate security policies and procedures, including systems and controls for the ongoing monitoring of their security.
- provide Data Breach reporting to their Data Holder partners.
- have contractual indemnity for data loss.

We refer to these Intermediaries as having a "direct data feeds". More than 1 million consumer bank accounts are currently accessed via direct data feeds in Australia[1]. SISS Data Services provides access to over 350,000 accounts via Direct Data Feeds.

Intermediaries that use screen-scraping instead of direct data feeds typically operate without agreements in place with Data Holders, and have no accountability in the form of fine-grained consent to access only specific accounts. Intermediaries using screen-scraping are also not compelled to:

- Undertake background checks of staff members
- Maintain certain levels of insurance
- Adhere to security best practices (such as those required as part of CDR Accreditation)

[1] SISS Data Services, MYOB and Xero are the main users of Direct Data Feeds in Australia.

3. Trusted Advisers

SISS Data Services supports the concept of sharing data under the Trusted Adviser disclosure. However we draw attention to 3 key areas:

1. The practical implementation of the Trusted Adviser process needs to ensure that compliance burden is not added to the Adviser.
2. Initial due diligence of Trusted advisers should ensure that fraudulent activity is minimised or removed from CDR data sharing with Trusted Advisers.
3. Consumer protections should not be weakened in an attempt to share data.

Compliance burden should not lie with Trusted Advisers

Background

Under the proposed rules a CDR consumer can consent to an Accredited Data Recipient (ADR) to disclose CDR data with a Trusted Advisers provided that the ADR "has taken reasonable steps to confirm that the trusted adviser is currently a member of a class of trusted advisers mentioned".

We refer to this due diligence process undertaken by the ADR as 'Trusted Adviser Vetting'.

The Issue

We believe the use of the term 'reasonable' is ambiguous and detailed clarification as to what is considered as reasonable steps need to be provided by the Treasury. Additionally, we also highlight the following issues:

1. Customer protection under the proposed Trusted Adviser disclosure relies on the adviser themselves be part of and continues to be a part of a professional association. However, the Trusted Adviser Rule is silent about the situation where a Trusted Adviser becomes de-listed from professional registration part way through a year.
2. The Rules also do not provide for de-identification of data by Trusted Adviser. That is to say, if after data is shared with Trusted Adviser, and the professional is de-listed from the professional register, there is no way to ensure that the CDR data of consumer shared is deleted by the professional and not used for unauthorized purposes.
3. Bad actors could obtain CDR data fraudulently under a Trusted Adviser disclosure if proper due diligence is not undertaken.
4. Since ADRs are expected to verify Trusted Adviser every time before disclosing data will the Treasury arrange for or provide for a professional register which ADR can have quick access to verify status of Trusted Adviser?

Without there being a detailed guideline on due diligence process for verifying Trusted Adviser undergoing identity checks, the Trust Adviser disclosure provides an easy platform for fraudulent participants to enter the CDR environment.

Our objective

To ensure there is clarity around the Trusted Adviser vetting, frequency of such auditing and reduce the chance of fraud and misuse of CRD data.

What we propose

We propose the rules require an ADR to take the following steps, prior to disclosing data with a Trusted Adviser:

1. Have a system in place that allows verification of the identity of the Trusted Professional as per the guidelines provided by the Treasury
2. Develop a system which allows for updating and verifying professional membership of Trusted Advisers no less than daily
3. ADR should provide training and support to Trusted Adviser acquainting Trusted Adviser with the CDR regime
4. Maintain a virtual and separate register for each Trusted Adviser

Why this is needed

The identity check and subsequent check against the professional membership records, reduces the chance of fraud and financial harm against the Consumer. Without Identity checks, bad actors could provide an ADR with publicly available details from a professional association and fraudulently obtain CDR data about a Consumer.

ADR creating and maintaining a register of Trusted Adviser Register ensures there is a formal process to check the eligibility of the Trusted Adviser before CDR data is shared.

Trusted Advisers status should be checked before consent

Background

As per the proposed Rules, one of the condition precedents for sharing data with Trusted Adviser is that an ADR is required to confirm that the person to whom the data is to be disclosed is a member of a class of trusted advisers as set out in the CDR Rules.

The Issue

The current proposal requires an ADR to verify each Trusted Adviser before disclosing data with the verified professional. However, the Rules do not provide for the frequency with which an ADR must check the status of the Trusted Adviser professional association status.

Our objective

To reduce the risk of CDR data being shared with a Trusted Adviser that is not part of a professional body.

What we propose

The rules require the ADR to:

1. Maintain an internal Trusted Adviser register and check the register to Trusted adviser eligibility prior to permitting a Trusted Adviser disclosure.
2. Ensure that a Trusted Adviser register is updated for verified and eligible members no less than daily.
3. Prior to granting a Trusted Adviser consent, ADR must check the status of Trust Adviser on an internal register.

Why this is needed

At the point of granting a Trusted Adviser consent, if the Trusted Adviser is no longer part of the professional association, the Consumer is not afforded the protections under the professional body.

As a minimum protection for the Consumer, the rules should provide for the ADR to create and maintain its own internal register of Trusted Advisers, which it must check prior to granting a Trusted Adviser consent.

Liability under this proposal

Where an ADR has created and maintained an internal Trusted Adviser registry, and approved consent in line with that registry, the ADR will not be liable for any harm caused to a Consumer.

Portability for Trusted Adviser vetting

Background

As per the proposed Rules, a condition precedent for sharing data with Trusted Adviser is that an ADR is required to vet/confirm that the person to whom the data is to be disclosed is a member of a class of trusted advisers as set out in the CDR Rules.

The Issue

Not all ADRs may have the technology, skills, and resources to implement a Trusted Advisor vetting process every time before disclosing data with the Trusted Adviser.

Our objective

The objective of this proposal is to provide ADR's with options on how they comply with the Trusted Adviser obligations and reduce compliance costs.

What we propose

The rules to permit an ADR to rely on another ADR's technological infrastructure for vetting a Trusted Advisor, by ensuring the following criteria has been met:

1. There is a written contract between the ADRs that will outline the responsibilities, warranties and liabilities of each party entering into the contract;
2. The vetting has been performed in accordance with the rules;
3. ADRs can provide for vetting either for all Trusted Advisers or just one of the classes of Trusted Advisers, depending upon the ability of the unrestricted ADR;
4. Invite the Treasury to determine eligibility criteria for ADRs which can qualify to provide such vetting services for other ADRs. The eligibility criteria should importantly determine skills and technical resources required to qualify as an ADR for providing vetting services;
5. There is a mandatory risk management framework to manage the vetting process with 3rd parties;
6. Such other requirements which the legislator may require for the success of this proposal.

Why this is needed

Portability of the Trusted Adviser vetting will reduce the need for Trusted Advisers to be vetted with multiple ADR's (repetition) and reduce the cost of Trusted Advisers to comply with CDR rules.

Liability under this proposal

The ADR performing the vetting and providing such service would be liable only to the extent where they failed to vet the Trusted Adviser in accordance with the rules. Accordingly, the success of this proposal depends on the fact that the Treasury provides for detailed guidance on what reasonable steps are required to be undertaken for verifying the Trusted Adviser.

Worked Example 1

Giant Automation is an Accredited Data Recipient (ADR) and has built an efficient system for vetting Trusted Advisers. Giant Automation vets Trusted Advisers for an annual fee and makes their status available to other ADR's via an API.

AAA Accounting software is accounting Software Provider (ASP) and needs to vet Trusted Advisers before they can disclose data but does not have the systems or processes to vet Trusted Advisers.

Giant Automation enters in a written contract with AAA Accounting software to vet Trusted advisers. AAA Accounting Software's trusted Advisers go to be vetted. Giant Automation completes the process and AAA Accounting access the result via the API.

Worked Example 2

Phillip is an Accountant and he uses multiple Account Software Providers (ASP) to provide services to his customers. New Age Accounting Software requires Phillip to go through the vetting process for Trusted Advisers. Phillip instructs New Age Accounting Software to obtain its verified professional status from Giant Automation as Philip has already been verified under Giant Automation's vetting process, which is a Treasury defined vetting process.

4. Add-ons

Add-ons play a vital role within a FinTech's eco environment to provide functionality and compliance.

Portability of accreditation for Add-ons

Background

Many Fintechs ("Parent Company"), such as Accounting Software Provider (ASP) have add-ons, where additional functionality can be "plugged in", they are commonly referred to as add-ons. Add-ons provide extended services for parent company. For instance, Fathom Reporting (www.fathomhq.com) which is an Addon for QuickBooks, MYOB and Xero provides management reporting.

Add-ons are an integral part of the overall eco environment and will need to comply with the CDR rules since they will require CDR data to provide services to their consumer. While some add-ons will be able to operate under the CDR insight rules, many will need to be accredited. Given the cost involved and technological support required to secure accreditation not many add-ons are likely to seek/receive full CDR accreditation. This in turn would leave a significant group of participants out of scope for access to CDR regime.

Should an Add-on be associated with one ADR (sponsorship model) they may need to be associated again should they provide a service with another ADR.

The issue

Fintechs with add-ons need:

- To reduce the cost of participating in the CDR system, and/or;
- a way to sponsor and provide CDR data to their add-ons which they rely on. They therefore need a model that allows transfer of data between FinTechs and their add-ons.

The current sponsorship/ model does not provide for extending benefits of sponsored accreditation to addons.

This means the FinTech must incur the cost and complexity of applying for an unrestricted level of accreditation and ensure they systems and resources to manage the accreditation for the add-ons.

What we propose

We propose for a provision in the sponsorship model that allows such add-ons to be a part of the CDR environment through the app-eco environment, which will be accredited to sponsored level.

How this can be achieved

An unrestricted ADR which provides sponsorship to affiliate, would conduct an independent third party audit of information security control and privacy safeguard implemented by such add-ons of the affiliate. The audit would not only cover data security control measures which the add-on is required to have in place, but also such other eligibility criteria as explicated under Rule 5.12. Additionally, the Treasurer can provide the independent auditor category through such third party audit should be conducted by the ADR, before it provides sponsorship to such add-ons. If the add-ons satisfy the conditions as mentioned above, the unrestricted ADR can extend and replicate its CDR services to such add-ons.

The liability framework

Given that such add-ons are primarily an extension of affiliate and the affiliate would be extending their sponsorship with add-ons, the liability model should be similar to that of sponsorship model, which is shared between the affiliate and sponsor. Certainly, the add-ons and affiliate (the parent company of such add-ons) can have an internal agreement in place for duties and liabilities of each of the party, in such situations.

Why this is needed

It enables an add-on associated with a FinTech with an extended eco environment to participate in the CDR under a sponsorship agreement.

5. Sponsorship Model

Affiliate Training and assistance under Sponsor's obligation

Background

Under the proposed Rules, one of the obligations of a sponsor under Sponsorship model is to provide to its affiliate any appropriate assistance or training in technical and compliance matters.

The issue:

The proposed Rules do not elucidate upon the several key issues pertaining to providing training:

- Whether the sponsor can outsource such responsibility to third party
- The period/ frequency with which such training is to be provided
- The scope of the training and assistance provided
- What specific evidence are the ADRs required to maintain towards providing training

What we propose

We propose that the Treasury provides more clarity and elaborate in detail upon the issues raised above and such other points that would enable providing training and assistance in a detailed manner.

Why this is needed

While determining liability, such clarity will enable ADRs to understand if the sponsor has met the obligations appropriately regarding training and assistance of the affiliate.

Format and requirements of self-assessment process

Background

Under the proposed Rules, the accreditation criteria for sponsored accreditation requires an affiliate to provide a self-assessment and attestation to the Data Recipient Accreditor.

The issue

The issue/ limitation that we observe in the proposed Rules is that insufficient information is provided on the format of self-assessment or the items which are mandatory requirements of the self-assessment process.

Absence of clarity in the Rules keeps it wide open for CDR participants to develop a third-party framework or conduct self-assessment at their own convenience, which may not assure safety and security and thereby undermine the consumer protection strength of the regime.

What we propose

With regards to self-assessment process, we request the Treasury to provide more clarity on items such as the format of self-assessment and items which form a mandatory part of self-assessment criteria, which cannot be compromised by the affiliate.

Why this is needed

We make this proposal to understand the scope of obligation of both the sponsor and affiliate. By providing clarity on self-assessment framework, affiliate would understand the extent of disclosure they need to provide, which will in turn enable sponsor to understand if they are legitimate and secured enough to enter into a sponsorship agreement with.

6. Additional points of Considerations for Treasury

The Treasury is also asked to consider and reflect upon the following situations:

1. Enabling Add-ons to seek CDR services from multiple ADRs

Treasury should consider a situation where an add-on can seek CDR services from more than one unrestricted ADR. This can be done through an existing unrestricted ADR of the add-on providing confirmation to the new ADR regarding the information and security control levels of the add-on. The new ADR can in addition to this confirmation also conduct a due diligence of its own before agreeing to sponsor the add-ons.

2. Integrating Trusted Advisers and Representatives in a Representative Model

Given that Rules pertaining to Trusted Advisers only allow Accredited Persons to invite CDR consumer to nominate Trusted Adviser, this creates an obstacle for Representatives to share data with Trusted Advisers, since most representatives will be unaccredited and thus cannot invite consumers to nominate Trusted Advisers for disclosing data with them. Since the objective of the Trusted Adviser model was to increase participation of professionals in the CDR regime, this becomes unachievable under the current scenario which allows only "accredited person" to disclose data with Trusted Adviser.

Accordingly, the Treasury is asked to provide clarification/ solution in such a scenario where Representatives will be allowed to disclose data with Trusted Advisers and integrate Trusted Advisers in their ecosystem.

3. Allowing unaccredited OSPs to collect data undermines the CDR regime

We believe that the provision allowing unaccredited OSPs to '*collect data'* from data holders is highly contentious for the following reasons:

Undermines the objective of the legislation

The underlying aim of the Consumer Data Right is to *"give consumers greater access to and control over their data and will improve consumers' ability to compare and switch between products and services."* Accordingly, to ensure consumers can control the safe disclosure of their data, collection of data should be reserved for accredited OSPs. This is because collection of data is the first point through which data leaves the security regime of data holders and is provided to an external environment. Therefore, consumers should have the ability to provide their data from one safe regime to another. Although Rule 1.10 requires providers to take the steps in Schedule 2 to protect the service data as if it were an accredited data recipient, **the requirement under this provision is not subject to civil penalty law provisions**, thereby providing an easy escape for service provide to not comply strictly with the provisions in the said Rule.

Creates an un-level playing field

From service provider's point of view, allowing unaccredited OSPs in the system would discourage other service providers from obtaining accreditation as there is no advantage to accreditation. Moreover, those undertaking accreditation will be incurring an extra cost which will in turn increase the cost of their services too. This in turn puts accredited service providers at a competitive disadvantage.

Liability of principal is insufficient to hold OSP responsible

Even though the principal is liable for the acts of the OSP, it is not enough to ensure integrity, stability, and security of the system. This is because in the consequences of breach of data protection by OSP, the principal would only be liable for civil penalty provision. To reflect the

importance of protecting consumers' data in circumstances where principal is required to be held liable, their liability should be greater, such as revocation or suspension of the ADR's license.

Responsibility of regulator in identifying the status/legality of unaccredited OSPs

Making principals liable for the acts of the OSPs is not sufficient to ensure protection for the reasons listed above. We believe that the regulator should also be held accountable for ensuring some level of identity check before allowing unaccredited OSPs to enter the regime.

Conclusion

In conclusion, what we present is that, although enabling an accredited person to rely on unaccredited outsourced service providers to collect CDR data would reduce the cost of building and operating application programming interfaces, this will come at the cost of compromising data security and integrity. Furthermore, it will also discourage legitimate service providers to comply with strict accreditation rules.