SISS DATA SERVICES
OPEN BANKING API

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

Submitted February 2020

Contents

About SISS Data Services

SISS Data Services has been providing an open data solution as an Intermediary to FinTechs for ten years. SISS does not screen-scrape data. To deliver our service, we strongly believe in securely transferring only specific consumer consented data to the specified SISS partner.

There are aggregators (who are possibly Intermediaries) that access consumer data via screen scraping. These providers tend not to partner with Data Holders and have no accountability in the form of:

- Fine-grained consent to access only specific accounts
- Background checks of staff members
- Insurance
- Adhering to security best practices such as those required as part of CDR Accreditation
- Data Handling Policies and Procedures

There is another group of Intermediaries, such as SISS Data Services, who do partner with Data Holders and take their rights to access Consumer data very seriously. In this case, access to consumer data is access directly from the Data Holder, following the Privacy Act. Data Holders only grant data access once the Intermediary has proven:

- They have a robust consumer consent process (not screen scraping) which only allows access to specified accounts.
- Have undergone review(s) of their Security and their Policies and Procedures.
- Have 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 feed”.

More than 1 million accounts are accessed via direct data feeds[1]. SISS Data Services provides access to over 350,000 accounts via Direct Data Feeds.

While the terms Intermediaries and Outsourcers have been used frequently within the CDR discussion, SISS feels there needs to be a subtle but critical distinction made between Intermediaries, Outsourcers and Software Vendors.

[1] SISS Data Services, MYOB and Xero are the current Direct Data Feed users.

Difference between an Accredited Intermediary Service, an Outsource Provider & a Software Vendor

- An Accredited Intermediary Service exists between a Data Holder and a Data Recipient providing the infrastructure which collects Consent and makes data available to a Data Recipient.
- An Outsource Provider is a service an Accredited Data Recipient uses in providing part of the Accredited Data Recipients service which requires them to ship CDR Data to the Outsourcers environment.

E.g. an external Credit Scoring engine, which needs to have the CDR Data to perform its analysis. The Accredited Data Recipient supplies the Credit Scoring engine with data they have collected from the Consumer to have the Consumers Credit Score calculated.

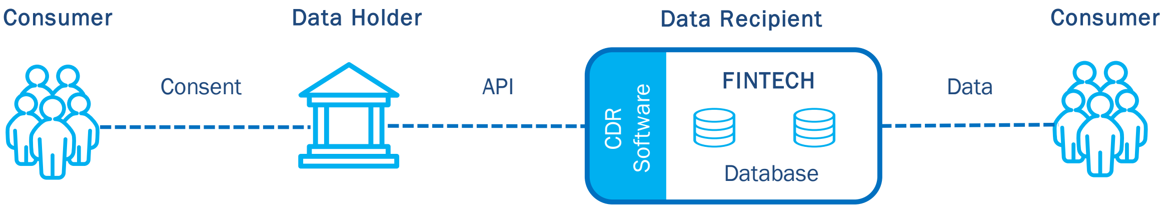
- A Software Vendor provides a solution which is installed in the Accredited Data Recipients environment, and provides some functions using the CDR Data in the Accredited Data Recipients environment.

E.g. a Software Vendor may be providing the engine to collect CDR Data from an Accredited Data Holder.

OR

A Software Vendor may be providing a credit scoring engine which is installed in the Accredited Data Holders environment, which works off the CDR Data held only in the Accredited Data Holders environment

What is a Software Vendor?

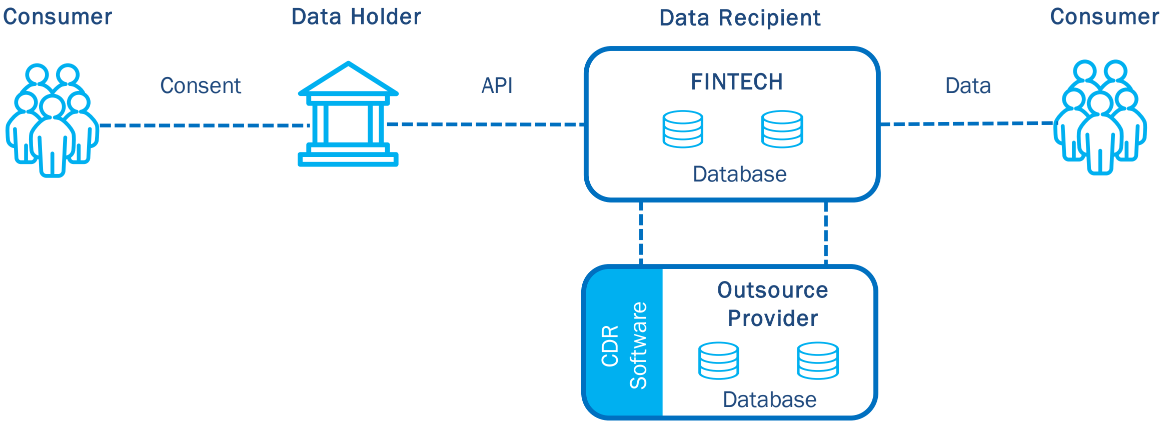


A Software Vendor provides an Accredited Data Recipient (ADR) with CDR software, or software which acts on CDR Data, which is installed and operated within the ADR's own environment. CDR data does not leave the ADR environment.

A Software Vendor only needs to ensure their software conforms to any relevant CDR Technical Standards, i.e. an API provider ensures that their APIs produce results compliant with the formal standards.

The Software Vendor DOES NOT need to be disclosed to the Consumer, as the Consumers data never leaves the ADR's environment.

What is an Outsource Provider?

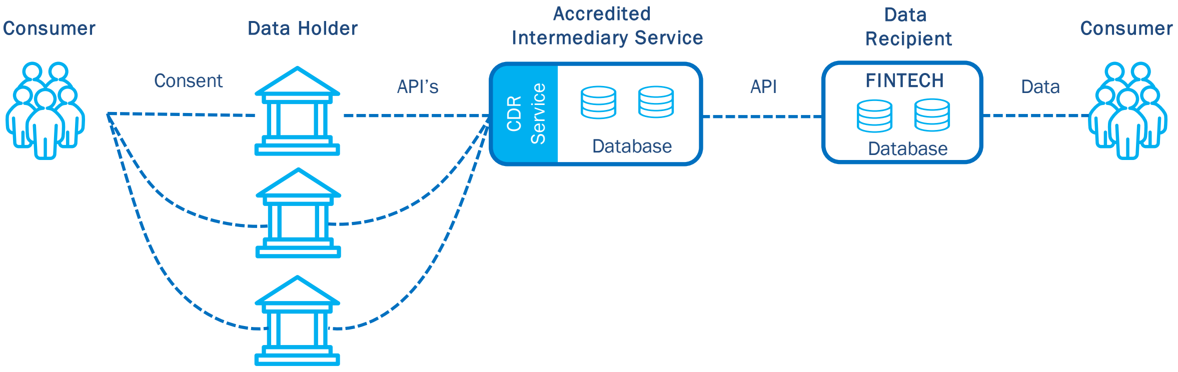


An Outsource Provider (OP) performs functionality that requires CDR Data to work. The ADR transfers the required CDR Data to the Outsource Providers environment and obtains result(s).

The Outsource Provider MUST be fully accredited as they are obtaining and processing CDR Data, and they may also be storing it depending on the requirements.

The Outsource Provider MUST be disclosed to the Consumer, as the Consumers data leaves the ADR's environment and may be stored with the Outsource Provider.

What is an Accredited Intermediary Service?



An Accredited Intermediary Service provides the infrastructure for a Data Recipient (Accredited, Restricted or Other) to participate in the CDR Environment.

The AIS can:

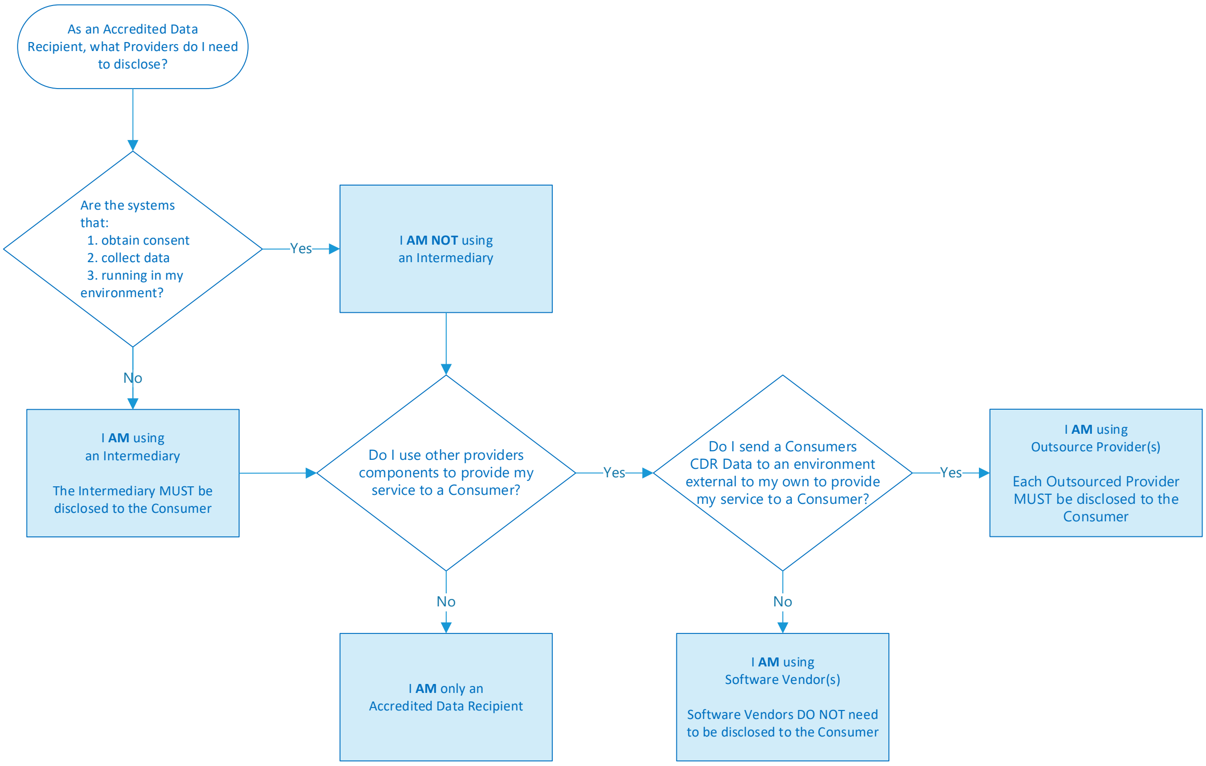
- Transfer the required Consumers consented data to an ADRs environment.
- Transfer the required Consumers consented RESTRICTED data set to an RDRs environment
- Provide ONLY a calculated result on the Consumers consented data to a Data Holder who is not an Accredited or Restricted Data Holder.

The Accredited Intermediary Service MUST be fully accredited as they are obtaining and processing CDR Data, and they may also be storing it depending on the requirements.

The Accredited Intermediary Service MUST be disclosed to the Consumer, as the Consumers data will be transiting through the AIS's environment and may be stored there depending on the requirements.

Data Recipient External Provider Disclosure Decision Tree

Should an Accredited Data Recipient be utilising the services or solutions of an external provider, how should they be disclosed to the consumer? We are putting forward the following decision tree.


As an Accredited Data Recipient, what Providers do I need to disclose?
Are the systems that:
1. obtain consent
2. collect data
3. running in my environment?
Yes
I **AM NOT** using an Intermediary
No
I **AM** using an Intermediary
The Intermediary MUST be disclosed to the Consumer
Do I use other providers components to provide my service to a Consumer?
Yes
No
I **AM** only an Accredited Data Recipient
Do I send a Consumers CDR Data to an environment external to my own to provide my service to a Consumer?
Yes
I **AM** using Outsource Provider(s)
Each Outsourced Provider MUST be disclosed to the Consumer
No
I **AM** using Software Vendor(s)
Software Vendors DO NOT need to be disclosed to the Consumer

Our approach to this Submission

When preparing this submission, we consulted with several Data Holders (Banks), that currently supply of data to SISS to understand their position regarding Intermediaries. We also consulted with several of our FinTech customers wanting to access CDR data to get a view on how Intermediaries can assist them as Data Recipients.

Consumer Data Security & Privacy

We believe that any changes to the CDR rules to accommodate Intermediaries should not compromise data security or privacy protections afforded to consumers under CDR

Technical Reference

When providing our feedback, we have considered the current CDR technical framework and understand that making changes to technical frameworks can be difficult. We believe our proposal has minimal impact.

Extension of Intermediary services to Data Holders

While this consultation paper is related to the use of Intermediaries for Data Recipients, the ACCC should also consider the extension of CDR rules to cover the use of Intermediaries for Data Holders.

Intermediaries give Data Holder options around how they comply with their CDR obligations.

1. Reduce the cost of complying with Consumer Data Right obligations
2. Speed to market to share or access CDR Data
3. Drive the economic benefit

For Data Holders, the costs of implementing a CDR compliant data sharing platform can be high. Concerning Open Banking, Westpac has quoted it would spend over 200 million dollars on implementing their Open Banking system[2].

While many Data holders do have the resources to deliver a secure and robust data-sharing platform, the ACCC will need to consider all Data Holders when developing CDR rules for Intermediaries. This will ensure unfair pressure is not placed on smaller Data Holder, especially those which are not- for-profit or member-based. Examples would be community-owned banks and superannuation funds, where the potentially high costs of CDR compliance would directly can directly affect the services to members.

[2] zdnet.com/article/westpac-predicts-open-banking-to-cost-au200m-to-implement/

Glossary of Terms

ADR	Accredited Data Recipient
CDR	Consumer Data Right
RDR	Registered Data Recipient
DR	Data Recipient
AIS	Accredited Intermediary Service
API	Application Programming Interface
CAPEX	Capital Expenditure
OP	Outsourced Provider
PCI DSS	Payment Card Industry Data Security Standard

Executive Summary

Response to ACCC Questions regarding Intermediaries

ACCC Question	Our Response
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 how best to facilitate the participation of principle service providers 4 Intermediaries can bring to the CDR regime and for consumers?	We intend to be an Intermediary Service for Data Recipients where we intend to collect and use consumer data, based on the purpose of the third party. The economic values we provide are • As a pre-built service, we reduce the development and setup cost of data recipients • As a pre-built solution, we improve the speed to market for data recipients • As part of our service, we reduce ongoing maintenance & compliance costs as we keep the services up to date with the CDR specifications • We can provide data recipients expert knowledge, experience and coaching to ensure they met the proper standards • We provide a data recipient a simpler development environment. They develop to a single provider and we maintain the connections to many data holders. • As an accredited solution we ensure data sharing remain secure and we accept responsibility (liability) for the solutions we provide • We can collect consumer data and allow non accredited data recipients run algorithms to gain a result, without exposing the raw consumer data to unaccredited parties • As an Intermediary we provide an upgrade path for a data recipient to start small (and therefore lower cost) and potentially grow into a full independent accredited data recipient. • As data sharing experts we assist data recipients be good actors by providing o Data breach reporting and management o Security and risk management o Customer compliant processes, procedures and dispute resolution
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.	CDR rules should provide for both Outsource Providers and Accredited Intermediary Services to drive adoption of the CDR system. CDR rules need to permit: • Accredited Data Recipient (ADR) to use Outsource Provider(s) (OP) under contract to provide various add-on services related to CDR Data. The outsource provider is audited and accredited to the same level as an ADR for services which use the provided CDR Data. • Accredited Data Recipient (ADR) to use an Accredited Intermediary Service (AIS) to retrieve CDR Data. The AIS service is audited and accredited and shares compliance and liability with the ADR.

ACCC Question	Our Response
What obligations should apply to Intermediaries? For example, you may wish to provide comment on: a. 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; b. if Intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and Intermediaries. c. if the obligations should differ depending on the nature of the service being provided by the Intermediary.	**Accreditation Requirements** For Intermediaries: an Accredited Intermediary Service (AIS) will attain the unrestricted level of accreditation as they provide CDR infrastructure and share liability with and ADR, including an ASAE 3150 audit. **Contractual Requirements** For Intermediaries – We are proposing a CDR accreditation tier for Intermediaries called Accredited Intermediary Service (AIS). We propose the rules permit the AIS to be liable to all CDR participants for the CDR services they provide.
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.	An Accredited Intermediary Service (AIS) ***MUST*** be disclosed to a Consumer as part of the consent process. The consent process for AIS ***MUST NOT*** require additional consent steps additional registrations or one-time passwords. Utilising an AIS ***SHOULD NOT*** add unnecessary friction for a Consumer. See SISS InVision CDR Consent Flow

ACCC Question	Our Response
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.	We believe data disclosure should only occur with explicit consent from the consumer. Disclosure of data requires consent regardless of the flow 1) Data Holder to accredited person 2) Accredited person to accredited person 3) Data holder to accredited person via an Intermediary If a consumer requests data deletion during the consent or withdrawal process, then all parties related to the consent have a requirement to meet that request. All parties should maintain logs of receiving the delete request and any processes they undertook to meet that consumer request. These logs can therefore be reviewed by auditors, reported to ACCC and presented to consumers in a dashboard. Should a CDR receipt be generated for the consumer, all parties, including Intermediaries and outsource providers, should be disclosed. Receipts could be generated for both the initial consent, re-consent and withdrawal.
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?	Yes - For an Accredited Intermediary Service (AIS) the ACCC should create a new tier in the Registry called a Registered Data Recipient (RDR) which MUST use the infrastructure of an Accredited Intermediary Service (AIS) to retrieve data. We believe this new tier will still met the current ACCC Security Requirements, the difference is around the use of Self-Assessment and Attestation over an External Auditor (similar to PCI DSS). Another key difference with the reduced tier is that an RDR receives a restricted data set, this basically matches the dataset that banks currently provide pre-CDR. Restricted means the RDR has a reduced auditing requirement by utilising the services and systems of an Intermediary. (see attached notes on our view of the restricted dataset) By enforcing the use of an AIS the new tier still maintains a high level of assurance, because both the AIS and RDR accept liability for their respective solutions.

ACCC Question	Our Response
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	The transfer of CDR data must between CDR Accredited Data Recipients/Accredited Intermediary Services and a Data Recipient registered with the ACCC. We propose a Restricted Data Recipient registration for Data Recipients who use an Intermediary and obtain a restricted data set. We also propose that Data Recipients who receive the result of a calculation run in an Intermediary's environment which is returning non-CDR Data should be registered, but have no Accreditation requirement
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?	None – The focus should be lowering the costs and restricting the data for lower levels of data recipients.
What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party	The transfer of CDR data must between CDR Accredited Data Recipients/Accredited Intermediary Services and a Data Recipient registered with the ACCC. We propose a Restricted Data Recipient registration for Data Recipients who use an Intermediary and obtain a restricted data set. We also propose that Data Recipients who receive the result of a calculation run in an Intermediary's environment which is returning non-CDR Data should be registered, but have no Accreditation requirement

ACCC Question	Our Response
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?	The transfer of CDR data must between CDR Accredited Data Recipients/Accredited Intermediary Services and a Data Recipient registered with the ACCC. We propose a Restricted Data Recipient registration for Data Recipients who use an Intermediary and obtain a restricted data set. We also propose that Data Recipients who receive the result of a calculation run in an Intermediary's environment which is returning non-CDR Data should be registered, but have no Accreditation requirement

About Intermediaries

What is an Intermediary

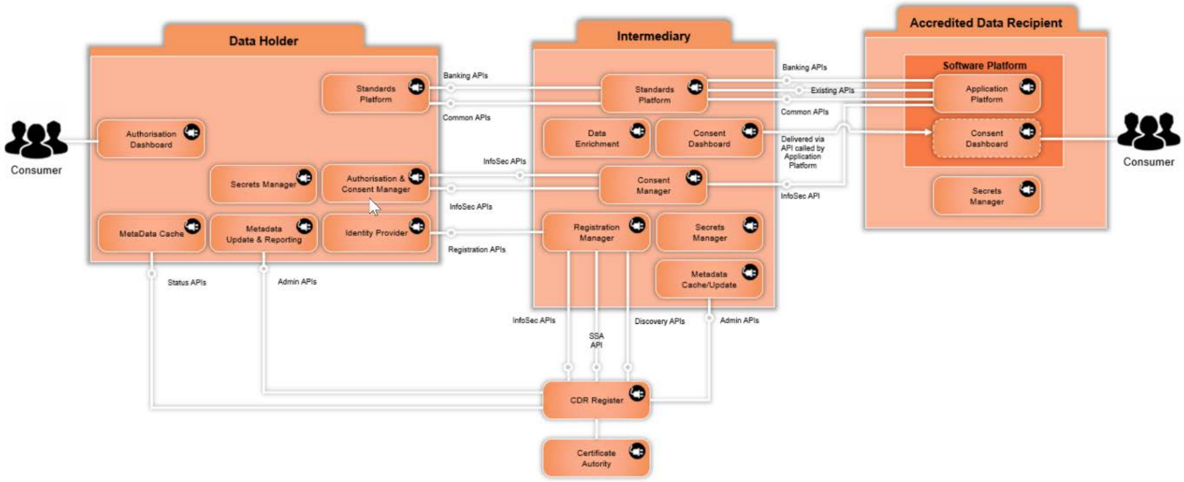
An Intermediary is a CDR participant that provides services and solutions to assist Data Recipients comply with their CDR Obligations within the Consumer Data Right (CDR) framework.

In this submission, we make a clear differentiation between an Intermediary, an Outsource Solution Provider and a Software Vendor.

What are the services an Intermediary can provide a Data Recipient?

Intermediaries provide access to CDR compliant infrastructure. The delivery of a prebuilt, secure, compliant and easy to adopt platform helps Intermediaries reduce the cost and compliance burden for Data Recipients.

Specifically, an Intermediary would provide some of or all the components in the following model:



A comparison of the use of an external provider (like Accredited Intermediary Service or outsourcing provider) and software solution provider is listed below:

	Accredited Intermediary Service (AIS) or Outsourcing provider	Software Solution
Description	An accredited CDR service provider for Accredited Data Recipients (ADR) to connect to (separate environment) to meet their CDR Data Recipient functionality and/or obligations.	A CDR software solution for Accredited Data Recipients (ADR) to deploy into their own environment to meet their CDR Data Recipient functionality and/or obligations.
Examples of the type of solutions or services provided	• CDR Consent • Consent Management • API connectivity to Data Holders • API connectivity to ACCC registry API connectivity for Data Recipient Data Breach Mgmt & reporting • Allows aggregation of data from multiple DH's into a single API call for an ADR • Security Monitoring & Mgmt • FICS membership (via AIS) • CDR Compliance Advice • Privacy Compliance Advice	• CDR Consent • Consent Management • API connectivity to Data Holders • API connectivity to ACCC registry API connectivity for Data Recipient • Connection into core backend solutions • Database management
Accreditation	Unrestricted – Must attain and maintain accreditation in their own right.	None – Software forms part of the Accredited Data Recipients (ADR) environment
Does this provider store, process or transmit data outside the Accredited Data Recipients (ADR) Environment	Yes – The Accredited Data Recipients connect to and access CDR data.	No - Software forms part of the Accredited Data Recipients (ADR) environment, CDR Data should only reside in the ADR Environment.
Liability	The AIS or Outsourcing provider has liability for the provision of it services to all CDR Participants	None – Accredited Data Recipients (ADR) is liable for the Software Solution.
Consent	External parties are to be disclosed during the Consent process as CDR Data is store, transmitted or proceeded outside the ADR environment.	None – Software solution forms Accredited Data Recipients (ADR) environment. Software solutions do not need to be disclosed
Contract	A contract is required between the ADR and the external provider	A contract is required between the ADR and the software provider.

What problems do Intermediaries solve for CDR

CDR Costs are Prohibitive

The costs for an unrestricted accreditation are prohibitive for Data Recipient. The costs are not just the initial build, compliance and audit costs which have been quoted between $100,000 -$300,000, it is also ongoing obligation, which we believe will require 1 full time equivalent employee + audit costs.

The Intermediary model we propose will reduce the costs for Data Recipients by up to 50%, please refer to **Schedule 1** for our costs and worked example.

Screen Scraping

Intermediaries provide FinTechs with an alternative to screen scraping. In our experience in sharing bank data over the last 10 years, we have yet to find a FinTech that would choose screen scraping over a direct, consented data feed.

The main drivers for FinTech using screen scraping have been:

- small cost
- simplicity of development
- less restrictive consent process
- difficulty/impossibility of directly contracting with banks (and many other data holders)

Intermediaries can solve the cost and complexity issues for FinTech's accessing CDR data by partnering with FinTechs to provide a cost-effective and easy to adopt the solution as an alternative to screen scraping and improve data security for Consumers.

SISS believes a properly implemented CDR system will allow FinTechs to collect data via an accredited CDR channel and eliminate the need for screen scraping. Ultimately this means a legislative sunset to the practice of screen scraping should be considered.

Multiple CDR Data use cases & Business Models

The CDR dataset and data use cases vary significantly between Data Recipients; therefore, CDR accreditation needs to take a flexible and not a "one size fits all" approach.

The business model for some Data Recipients will mean CDR data is core functionality; for example, loan approval, financial planning, budgeting, product comparison services.

For other Data Recipients, CDR data will be an addon or optional feature, for example, accounting software, CRM solutions (client relationship management).

There are also business models where the data recipient does not need access to the raw CDR data, rather they run an algorithm over the data to achieve a specific result and the underlying consumer data remains with the Intermediary.

Intermediaries can cater for multiple data use cases and business models such as restricted data sets, allowing Data Recipients to perform calculations on CDR Data without directly accessing or storing data or simply plug and play CDR infrastructure.

Data holders become a Data Recipient

Under the current guidelines an ADI, i.e. Data Holder will meet the criteria for a streamlined accreditation as a data recipient. While becoming a data recipient is attractive to all data holders, this is not economically viable for many the of smaller banks and mutuals (customer-owned banks).

This means a key outcome of the CDR system is not achieved, an equal playing field for all data holders and data freedom for consumers. Intermediaries can provide an off the shelf solution to get customer consent & collect data. These off the shelf solutions will provide data holders with a choice to utilise a cost-effective solution and enable quicker deployment of their data recipient capabilities. Key benefits of an Intermediary's solution are

- A pre-built and accredited solution has a significantly lower CAPEX expense
- The cost to maintain an ADR system is reduced and requires fewer resources by the bank as the Intermediary handles many functions
- The time to build a consent and data collection system is reduced. These data holders only need to build a single connection to the Intermediary, the Intermediary then manages the connections to multiple data holders (across banking and all future designated industries)
- Management of compliance and reporting is the responsibility of the Intermediary

This issue will become more prevalent as other industries become designated Data Holders. Many future data holders will not have the resources to implement their data holder or data recipient functionality. Meeting their CDR requirements requires an upfront and ongoing cost, more importantly, these data holders require resources and skillsets that do not core to their business. The role of an Intermediary is to be a data expert; therefore the value proposition exists for Data holders and recipients to utilise the services of Intermediaries.

Intermediary Accreditation

What level of Accreditation should an Intermediary hold?

The Intermediary ***must*** attain unrestricted accreditation to participate in the CDR Environment. The main reasons for

1. Intermediaries are a high concentration point for CDR data flow
2. Intermediaries connect to Data Holders and the ACCC Registry

Additional Controls and Compliance for Intermediaries

In addition to meeting all the same controls of an unrestricted Accredited Data Recipient, an Intermediary should have processes and contracts for onboarding Data Recipients, similar to the requirements which are a part of ISO 27001.

An Intermediary has a responsibility within the CDR program to ensure that only appropriate lower-tier data recipients obtain registration and access to CDR data. If a Fully Accredited Data Recipient wishes to access data via an Intermediary, then these processes are much more streamlined.

Accreditation Tier for Intermediary

To ensure traceability and transparency, we recommend a new tier of accreditation noted as an Accredited Intermediary Service (AIS).

How Intermediaries can help manage or reduce risk

Intermediaries help manage and minimise the risk to the CDR regime for lower-tier Data Recipients by providing a process of appraising the capabilities of these lower-tier Data Recipients and assume some responsibility for them having access to data. During this process, an Intermediary will assist a lower-tier Data Recipient to ensure that they have appropriate security controls in place, in alignment with the CDR security requirements which would be the subject of an ASAE 3150 audit.

Intermediary Services for Data Recipients

An Accredited Intermediary Service (AIS) will drive the adoption of Open Banking by reducing the cost, complexity and compliance for FinTechs to access CDR Data.

What Services does an Intermediary provide a Data Recipient?

CDR Access Platform

Prebuilt, easy to adopt platform for Data Recipients to access CDR data

Data Breach Management

System for Data Recipients to report and manage any data breaches

Data Security

System to report results of penetration testing, vulnerability scans, malware, antivirus & data loss prevention

Complaint Handling

Systems for Data Recipients report and manage consumer complaints

Cyber & PI Insurance

System for Data Recipients to provide evidence PI & Cyber insurance and certificate of Currency

		Mandatory	Optional
Application Platform with the following Functionality:			
	Connect to Data Holder APIs	✓	
	Allow Data Recipient to communicate with the AIS	✓	
	ACCC Registry or Data Holder to communicate with the AIS	✓	
	InfoSec API (e.g. for removal of the consent)	✓	
	Secrets Management	✓	
	Registration Management	✓	
	Metadata	✓	
	Data Enrichment		✓
	Data Calculations		✓
Compliance, Legal services & Data Security			
	Data Breach Management and Reporting		✓
	Consumer Dispute External Dispute resolution for		✓
	Insurance		✓
	Vulnerability Scanning		✓
	Penetration Testing Services		✓
	Compliance Breach Reporting		✓
	Privacy Policy & Privacy Impact Assessments		✓

Why would a Data Recipient use an Intermediary?

Key drivers for Data Recipients to use an Intermediaries

1. They may not wish to commit to the upfront costs of building or the ongoing costs of maintaining the infrastructure to participate in CDR. They may choose to use an Intermediary's compliant infrastructure to do the work for them.
2. Is looking for a fast way to get up and running while they build out their infrastructure or complete the Accredited Data Recipient audit requirements.
3. Develop a single API connection to an Intermediary, who turn manages the multiple connections. Allows for a single call to collect all data from all DH's and for all consumers.
4. Does not want to be an Accredited Data Recipient, and only wants the restricted data set that an Intermediary can provide.
5. Does not want to be an Accredited Data Recipient, and only have calculations run on the data in the Intermediaries infrastructure, getting the returned result.
6. Lack of skilled resources. Not all DR have the economic capability to employee and maintain a full-time resource. Using the expertise of an Intermediary allows a DR to access systems, resources and knowledge not otherwise available.

Permitted Intermediary Data Sharing Models

In consultation with FinTechs we have identified the following use cases Accredited Intermediaries can facilitate:

Data Scope	Accreditation	Description	Example
Unrestricted Data	Accredited Data Recipient (ADR)	A solution where-by an Accredited Data Recent can outsource the collection of data via an Intermediaries pre-built, CDR Compliant infrastructure.	A large multination software vendor who doesn't have experience or knowledge of the Australian system and wishes to utilize a local partner to enable consumers to use their data.
Restricted	Registered Data Recipient (RDR)	An RDR receives a restricted data set, this basically matches the dataset that banks currently provide pre-CDR. Restricted means the DR has a reduced auditing requirement by utilising the services and systems of an Intermediary. (see attached notes on our view of the restricted dataset)	A start-up cloud-based practice management solution for Architects wish to connect to their customers' bank accounts to perform basic accounting functions and bank reconciliations. This start-up, in the short term, will only have 12 clients with 27 accounts, as such the combination of low volumes and basic data requirements means obtaining accreditation as an ADR is not economically viable.

Data Scope	Accreditation	Description	Example
Dual Data	Accredited Data Recipient (ADR)	ADR who wants to access some data holders or industries directly and then use Intermediaries for the balance of industries or data holders.	A cloud accounting software vendor wants to develop a connection and have relationships with the big 4 banks because they represent most of their customers. However, they don't wish to do the same with the remaining banks and develop a single connection to an Intermediary who in turn connects and manages the required, 20-80 banks.
No Data	Registered Data Recipient (RDR)	Where data does not leave the Intermediary. The Intermediary holds the raw data and a third party registers their routine with the Intermediary. The Intermediary ensures the routine doesn't expose CDR data to the third party.	An Income validation FinTech calls the Intermediary to run the registered routine which queries a customer's account looking for deposits from an employer. The data returned to this app would be the number of transactions in the last period (say 6 months) and the total value of these transactions. None of the raw data from the bank is visible or disclosed, only the calculated values are exposed. Another example could be an Auditor; their app requests the balance of an account as at a specific date, for example, 30th June the key reporting date for many audited entities.
Return Consumer Data	n/a	A way for consumers to access their data. The Intermediary could package up data in various formats from multiple banks, eg Spreadsheets, Text Files, XML or Database	An everyday customer who has accounts with five financial institutions. This service would allow them to have a single point to login to consolidate all accounts from all institutions and then view or download the data. Going forward the Intermediary & therefore consumer will have access to more data sources.

Accreditation tiers via an Intermediary

The following accreditation tiers are proposed via an Accredited Intermediary Service (AIS)

	Accredited Data Recipient (ADR)	Restricted Data Recipient (RDR)	Data Recipient
Usage of Accredited Intermediary	Data Recipient with full access to all CDR Data MAY use AIS to simplify their processes	Data Recipient wanting access to a limited data set MUST use AIS to access data	Data Recipient wanting to run an algorithm process over data held by Intermediary but not access or store CDR data MUST use AIS to access data
Scope of access to Consented CDR Data	Unrestricted access to any requested scope as part of the consent process.	ONLY Basic Account, or Basic Transaction (see appendix for our thoughts on the restricted dataset)	None
Access Methods	Directly or via Intermediary or both	Via Intermediary	Via Intermediary
Accreditation Type	Compliance	Attestation	Attestation
Disclosure to Consumer	Use of an Intermediary disclosed to Consumer during the consent process	Use of an Intermediary disclosed to Consumer during the consent process	Use of an Intermediary disclosed to Consumer during the consent process
Liability	Joint liability	Joint Liability	Joint Liability

Accreditation of Data Recipients via an Intermediary

Where a Restricted Data Recipient uses the services of an Accredited Intermediary Services (AIS) to access CDR based data. We believe an attestation approach rather than an external audit for accreditation is a better model.

Why the Attestation of Compliance?

Attestation of compliance is an existing, accepted and a proven model for providing flexibility for accreditation. We feel this approach should be adopted for a Restricted Data Recipients accreditation.

For example, The Payment Card Industry (PCI DSS) provides a tiered accreditation for merchants handling credit card data. The accreditation tiers are based on the number of transactions performed by the merchant. For the lower tiers, the process requires the merchant to complete a Self-Assessment Questionnaire followed by a declaration (Attestation of Compliance). At the top tier of PCIDSS, an Audit by an external party (a Qualified Security Assessor) is required.

For more information please refer to the following PCI link
https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

We've also marked up the "Draft Information Security Controls Guidelines" published by the ACCC in September, 2019 and included this in the appendix. Our mark-up is an indication of how we feel priorities could be set when determining the compliance of an RDR using the PCI DSS prioritised approach as a guide.

What are the benefits to a Customer of Data Recipients using an Intermediary?

For Consumer’s, the key benefits a Data Recipient using an Intermediary include:

Traceability - A consumer will have visibility as to where their data is being delivered and via what systems from the Dashboard at their Data Holder. The consumer will also know what data permissions are in place for specific data feeds.

This is in direct contrast to screen scraping, where the consumer only has visibility from the Data Recipients systems (if at all).

Management - A consumer can renew or disable data feeds from their Dashboard at the Data Holder, enabling them to terminate feeds to products that they no longer use.

This is in direct contrast to screen scraping, where the consumer only has visibility from the Data Recipients systems (if at all).

Constrained Exposure - A consumer specifically allows which accounts are exposed, and in the case of an RDR, the dataset made available matches what is available via direct feeds today.

This is in direct contrast to screen scraping, where any accounts associated with the login may be scraped, and transaction capability exists because they are impersonating the Consumer.

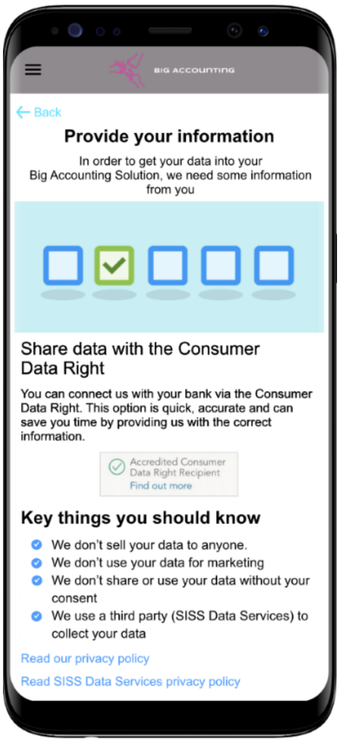
Disclosure of an Accredited Intermediary Service to a Consumer

For Data Recipients using an Accredited Intermediary Service (AIS) disclosure to the Consumer must be done when obtaining consent. While the Consent is between the Data Holder and the ADR/AIS, it should be transparent to the Consumer that data delivery is via an AIS. To provide these visual cues, it can be as simple as including AIS information within the consent flow.

See SISS InVision CDR Consent Flow

As a guiding principle, where CDR data is transferred or held outside of environments under the Data Recipients control, disclosure MUST be made in the consent process.

Data Recipient Consent screen when using an Accredited Intermediary Services



← Back

Provide your information

In order to get your data into your Big Accounting Solution, we need some information from you

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick, accurate and can save you time by providing us with the correct information.

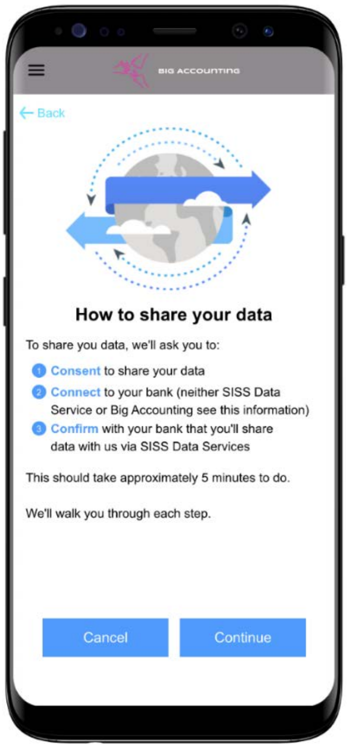
Accredited Consumer Data Right Recipient
Find out more

Key things you should know

- ✓ We don't sell your data to anyone.
- ✓ We don't use your data for marketing
- ✓ We don't share or use your data without your consent
- ✓ We use a third party (SISS Data Services) to collect your data

Read our privacy policy

Read SISS Data Services privacy policy



← Back

How to share your data

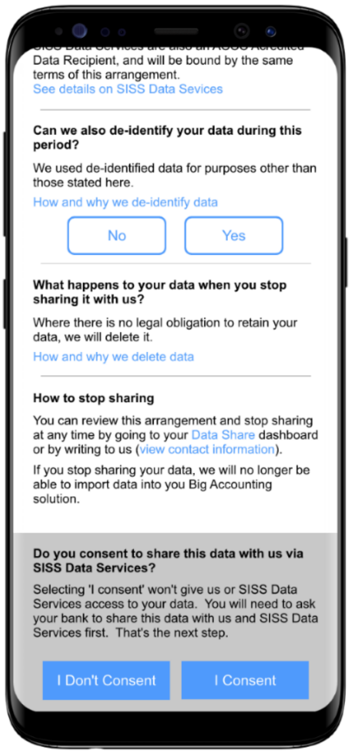
To share you data, we'll ask you to:

1. Consent to share your data
2. Connect to your bank (neither SISS Data Service or Big Accounting see this information)
3. Confirm with your bank that you'll share data with us via SISS Data Services

This should take approximately 5 minutes to do.

We'll walk you through each step.

Cancel | Continue


SISS Data Services are also an ACCC Accredited Data Recipient, and will be bound by the same terms of this arrangement.
See details on SISS Data Sevices

Can we also de-identify your data during this period?

We used de-identified data for purposes other than those stated here.

How and why we de-identify data

No | Yes

What happens to your data when you stop sharing it with us?

Where there is no legal obligation to retain your data, we will delete it.

How and why we delete data

How to stop sharing

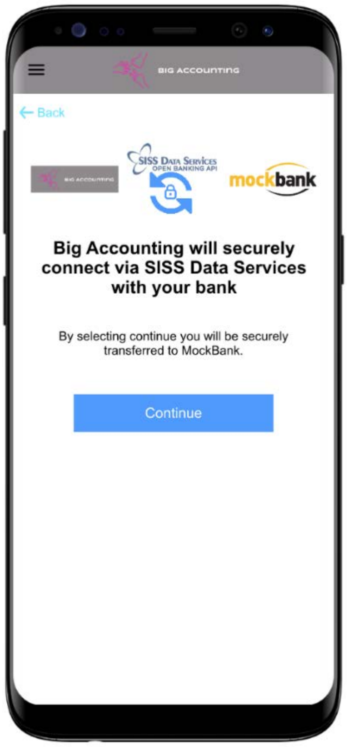
You can review this arrangement and stop sharing at any time by going to your Data Share dashboard or by writing to us (view contact information).

If you stop sharing your data, we will no longer be able to import data into you Big Accounting solution.

Do you consent to share this data with us via SISS Data Services?

Selecting 'I consent' won't give us or SISS Data Services access to your data. You will need to ask your bank to share this data with us and SISS Data Services first. That's the next step.

I Don't Consent | I Consent



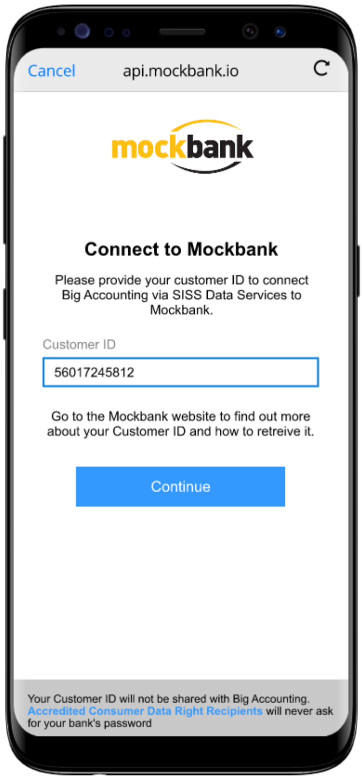
← Back

Big Accounting will securely connect via SISS Data Services with your bank

By selecting continue you will be securely transferred to MockBank.

Continue

Data Holder Consent Screens with AIS included



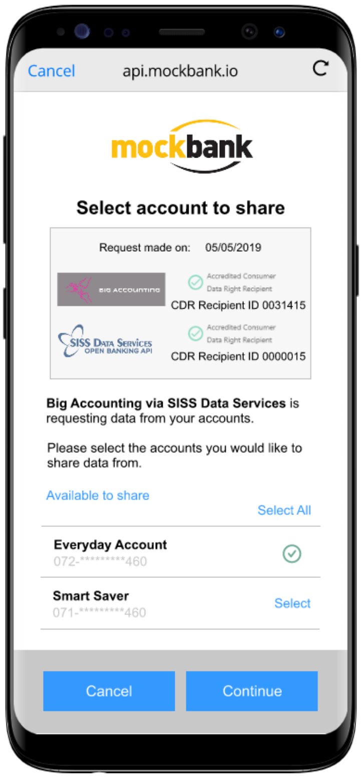
Connect to Mockbank

Please provide your customer ID to connect Big Accounting via SISS Data Services to Mockbank.

Customer ID: 56017245812

Go to the Mockbank website to find out more about your Customer ID and how to retreive it.

Your Customer ID will not be shared with Big Accounting. Accredited Consumer Data Right Recipients will never ask for your bank's password



Select account to share

Request made on: 05/05/2019

BIG ACCOUNTING — Accredited Consumer Data Right Recipient — CDR Recipient ID 0031415

SISS Data Services OPEN BANKING API — Accredited Consumer Data Right Recipient — CDR Recipient ID 0000015

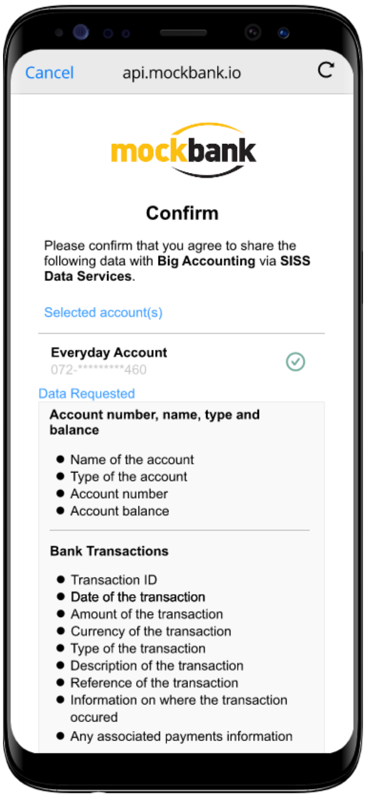
Big Accounting via SISS Data Services is requesting data from your accounts.

Please select the accounts you would like to share data from.

Available to share — Select All

Everyday Account 072-*********460 ✓

Smart Saver 071-*********460 Select



Confirm

Please confirm that you agree to share the following data with **Big Accounting** via **SISS Data Services**.

Selected account(s)

Everyday Account 072-*********460 ✓

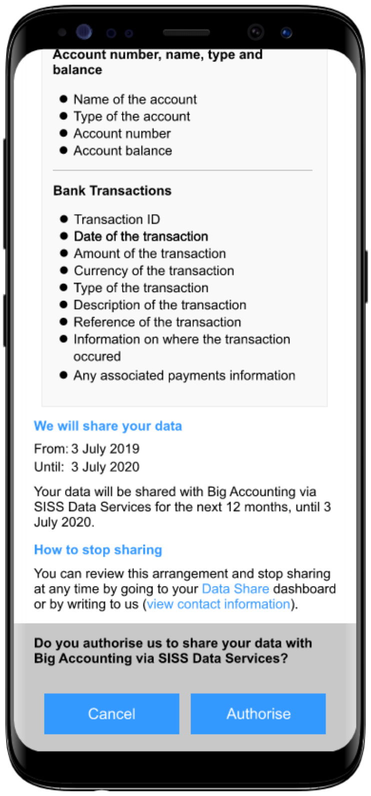
Data Requested

Account number, name, type and balance

- Name of the account
- Type of the account
- Account number
- Account balance

Bank Transactions

- Transaction ID
- Date of the transaction
- Amount of the transaction
- Currency of the transaction
- Type of the transaction
- Description of the transaction
- Reference of the transaction
- Information on where the transaction occured
- Any associated payments information



Account number, name, type and balance

- Name of the account
- Type of the account
- Account number
- Account balance

Bank Transactions

- Transaction ID
- Date of the transaction
- Amount of the transaction
- Currency of the transaction
- Type of the transaction
- Description of the transaction
- Reference of the transaction
- Information on where the transaction occured
- Any associated payments information

We will share your data

From: 3 July 2019
Until: 3 July 2020

Your data will be shared with Big Accounting via SISS Data Services for the next 12 months, until 3 July 2020.

How to stop sharing

You can review this arrangement and stop sharing at any time by going to your Data Share dashboard or by writing to us (view contact information).

Do you authorise us to share your data with Big Accounting via SISS Data Services?

Compliance Breach Reporting by Intermediaries

An Accredited Intermediary Service (AIS) is in a position of trust by CDR Participants; data holders, data recipients, consumers and regulators (ACCC). As such, they should be held to the highest accredited data recipient standards (as previously mentioned). Whilst an AIS are technically not auditors, they are in a position of having privileged information and insights regarding data recipients data compliance with CDR rules and guidelines. An AIS is well-positioned to participate in any implemented Compliance Breach Reporting system. This system would allow an AIS to report any compliance breach regardless of severity. These reports wouldn't necessarily be meant to be punitive but allow transparency which helps all parties to maintain a healthy ecosystem. As the regulator, the ACCC would have visibility over all breaches and can review reporting and intervene when necessary.

Does an Accredited Data Recipient share the product keys of a Data Recipient?

To maintain transparency, trust and accountability of an Intermediary to CDR participants, we suggest that Accredited Intermediary Services (AIS) be issued keys created under a product specifically for the ADR/RDR. Ideally, this product entry is linked to both the AIS and the ADR/RDR, enabling the clear identification of ownership and traceability of data.

The above approach also mitigates the situation for an ADR where they choose to collect data from some Data Holders themselves but use an AIS for others. It is always clear which systems the data has passed through, depending on the keys used. It also allows for data collection to be suspended or terminated via the AIS while not impacting the direct data collection by the ADR.

Requirements and standardised wording for these fields are defined by the Rules.				*SISS Suggested Priority*
1	An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment.	**Multi-factor authentication or equivalent control**	Multi-factor authentication or equivalent control is required for all access to CDR data.	1
2		**Restrict administrative privileges**	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.	2
3		**Audit logging and monitoring**	Critical events are identified, logged and retained to help ensure traceability and accountability of actions. These logs are reviewed regularly to identify irregularities and deviations from expected processing.	2
4		**Access security**	Processes, including automatic processes, are implemented to limit unauthorised access to the CDR data environment. At the minimum these include: (a) provision and timely revocation for users who no longer need access; and (b) monitoring and review of the appropriateness of user access privileges on at least a quarterly basis.	2
5		**Limit physical access**	Physical access to facilities where CDR data is stored, hosted or accessed (including server rooms, communications rooms, and premises of business operation) is restricted to authorised individuals.	1
6		**Role-based access**	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principles of least necessary privileges and segregation of duties.	2
7		**Unique IDs**	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained.	1
8		**Password authentication**	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history, and password ageing.	1
9	An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	**Encryption**	Encryption methods are utilised to secure CDR data at rest by encrypting file systems, end-user devices, portable storage media and backup media. Cryptographic keys are securely stored, backed-up and retained. Appropriate user authentication controls (consistent with control requirement 1) are in place for access to encryption solutions and cryptographic keys.	1
10		**Firewalls**	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: (a) restrict all access from untrusted networks; and (b) denying all traffic aside from necessary protocols; and (c) restricting access to configuring firewalls, and review configurations on a regular basis.	1
11		**Server hardening**	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.	2
12		**End-user devices**	End-user devices, including bring-your-own-device (BYOD) systems, are hardened in accordance with accepted industry standards.	1
13	An accredited data recipient must securely manage	**Data loss prevention**	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: (a) blocking access to unapproved cloud computing services; and (b) logging and monitoring the recipient, file size and frequency of outbound emails; and (c) email filtering and blocking methods that block emails with CDR data in text and attachments; and (d) blocking data write access to portable storage media.	1

Requirements and standardised wording for these fields are defined by the Rules.				*SISS Suggested Priority*
14	information assets within the CDR data environment over their lifecycle.	**Data in non-production environments**	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.	2
15		**Information asset lifecycle (as it relates to CDR data)**	The accredited data recipient must document and implement processes that relate to the management of CDR data over its lifecycle, including an information classification and handling policy (which must address the confidentiality and sensitivity of CDR data) and processes relating to CDR data backup, retention, and, in accordance with rules 7.12 and 7.13, deletion and de-identification.	1
16	An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	**Security patching**	A formal program is implemented for identifying, assessing the risk of and applying security patches to applications and operating systems as soon as practicable.	2
17		**Secure Coding**	Changes to the accredited data recipient's systems (including its CDR data environment) are designed and developed consistent with industry accepted secure coding practices, and are appropriately tested prior to release into the production environment.	2
18		**Vulnerability Management**	A formal vulnerability management program is designed and implemented, which includes regular vulnerability scanning and penetration testing on systems within the CDR data environment.	1
19	An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment.	**Anti-malware anti-virus**	Anti-virus and anti-malware solutions are implemented on endpoint devices and on servers to detect and remove malware from the CDR data environment and are updated on a regular basis. End-user systems are updated with the latest virus definitions when they connect to the network. Reports or dashboards highlighting compliance metrics are regularly generated and monitored, and non-compliant items are actioned as soon as practicable.	1
20		**Web and email content filtering**	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.	1
21		**Application whitelisting**	Download of executables and installation of software on infrastructure and end-user devices (including on BYOD devices) is restricted to authorised software only.	2
22	An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data.	**Security training and awareness**	All users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually.	3
23		**Acceptable use of technology**	A policy relating to the CDR data environment is created, implemented, communicated and agreed to by all personnel prior to being able to access the CDR data environment. This policy sets out the responsibilities of these personnel in interacting with the CDR data environment and is regularly made aware to personnel.	3
24		**Human resource security**	Background checks are performed on all personnel prior to their interacting with the CDR data environment. These may include, but are not limited to, reference checks and police checks.	3

Schedule 2, Part 2 of Rules				Additional guidance	Mapping				
#	Control requirements	Minimum controls	Description of minimum controls	Additional guidance	ISO 27001	PCI DSS	Trust Services Criteria	PCI Prioritised Approach Milestone	SISS Suggested Priority
1	An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment.	**Multi-factor authentication or equivalent control**	Multi-factor authentication or equivalent control is required for required for all access to CDR data.	Multi-factor authentication or equivalent control is required for access to all systems in the CDR Data Environment that collect, store, transmit, or modify CDR data. It should be noted that in some cases,a combination of location and office network may be considered as an authentication factor (one of the two required), such as if workstations are housed within an office or a user is required to be in the office (and hence gain physical access) to gain access to office network in order to log-in.		**8.3** - Secure all individual non-console administrative access and a remote access to the cardholder data environment using multi-factor authentication. This requires at least two of the three authentication methods described in 8.2 are used for authentication. Using one factor twice (e.g. using two separate passwords is not considered multi-factor authentication. This requirement applies to administrative personnel with non-console acces to the CDE (card holder data enviornment) from wtihin the entity's network, and all remote network access (including for users, administrators, and third-parties) originating from outside the entity's network.	**CC6.1** The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. **CC6.6** - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	2	1
		Restrict administrative privileges	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.	It is suggested that admin privileges be restricted in one of two ways: 1) users are not provided with ongoing administrative privileges. Rather, this is provided for a specified period of time only to perform specific duties. Once it is no longer required, acce is revoked; or 2) administrative privileges are limited to a small number of personnel on an ongoing basis. Administrative access rights is reviewed on a regular basis, at least monthly.	**9.2.3** - The allocation and use of privileged access rights shall be restricted and controlled. **12.4.3** - System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	**7.1** - Limit access to system components and cardholder data to only those individuals whose job requires such access. **8.7** - All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).	**CC6.6** - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	4	2
		Audit logging and monitoring	Critical events are identified, logged and retained to help ensure traceability and accountability of actions. These logs are reviewed regularly to identify irregularities and deviations from expected processing.	Critical events occurring within the CDR data environment should be logged and retained. A list of key events which may be used to detect malicious activity can be found at *https://acsc.gov.au/publications/protect/windows-event-logging-technical-guidance.htm*for Windows. Logs are for the dual purpose of identifying malicious activity to then address, and also in the case forensic analysis is required following an incident. Additionally, access to modify these logs should be highly restricted to prevent tampering	**12.4.1** - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	**10.2** - Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects.	**CC7.2 -** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	4	2
		Access security	Processes, including automatic processes, are implemented to limit unauthorised access to the CDR data environment. At the minimum these include: (a) provision and timely revocation for users who no longer need access; and (b) monitoring and review of the appropriateness of user access privileges on at least a quarterly basis.	This control pertains to the Joiners, Movers, Leavers (JML) process of securing logical access rights, and the performance of regular User Access Reviews. **Joiners:** Access rights to a system should be provided in line with the personnel's specific responsibilities. These rights should be approved by an appropriate person with sufficient knowledge of the system. **Movers:** When a user moves to a different role which requires different access rights, that users previous rights are revoked and new rights are provisioned in line with their responsibilities and approved by an appropriate person with sufficient knowledge of the system. **Leavers:** When a user leaves the organisation, all access rights previously provisioned to them should be revoked within a timely manner. This includes access to applications, databases, infrastructure and the network. A timely manner is at the discretion of the organisation, however in general should not exceed 2 weeks. **User Access Reviews:** On a regular basis, all access rights to systems within the CDR data environment should be reviewed by appropriate personnel with sufficient knowledge of the system. This includes a review of both whether the person is appropriate to have access (e.g. a legitimate user), and whether the provisioned access is appropriate (e.g. the roles and access rights match the user's responsibilities).	**9.2.2** - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. **9.2.6** - The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	**7.1 -** Limit access to system components and cardholder data to only those individuals whose job requires such access.	**CC6.2** - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. **CC6.3** - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	4	2
		Limit physical access	Physical access to facilities where CDR data is stored, hosted or accessed (including server rooms, communications rooms, and premises of business operation) is restricted to authorised individuals.	Physical access should be limited to only those personnel who are legitimately required to have access, given their responsibilities. Similar to the control on access security (which pertains to logical acess), an accredited data recipient should have defined JML processes for provisioning, modifying and revoking physical access to areas directly relevant to the CDR data environment. Further, a process for periodic review of access should be in place. However, where all or part of these processes are outsourced to an outsourced service provider, third-party assurance report should be sought. This control generally divides access into two parts: 1) d**ata centre:** Access to server rooms, and server racks; and 2) p**laces of business:** The premises at which an accredited data recipient primarily conducts their business operations.	**11.1.1 -** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. **11.1.2** - Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. **11.1.3** - Physical security for offices, rooms and facilities shall be designed and applied. **11.1.4** - Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. **11.1.5** - Procedures for working in secure areas shall be designed and applied.	**9.1** - Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. **9.2**- Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges. **9.3** - Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based on individual job function; access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled. **9.4** - Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and are asked to surrender the physical badge before leaving the facility or at the date of expiration. Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law. **9.5** - Physically secure all media; store media back-ups in a secure location, preferably off site. **9.6** - Maintain strict control over the internal or external distribution of any kind of media. **9.7** - Maintain strict control over the storage and accessibility of media. **9.8** - Destroy media when it is no longer needed for business or legal reasons. **9.9** - Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detec	**CC6.4 -** The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	1	1
		Role-based access	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principles of least necessary privileges and segregation of duties.	Role based access (RBAC) involves assigning specific access rights to a role and providing a user with access to that role as opposed to assigning rights directly to an account. This allows simplifes the user access management process. Further, RBAC should be used to minimise the access rights provided to each user to only that necessary for the user to perfor their assigned duties.		**7.2** - Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**CC6.3** - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	4	2
		Unique IDs	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained.	Generic, shared and default accounts should be limited to only those required to run a service or system. These accounts must have their password changed to a non-default password, and should be restricted to only necessary personnel. An accredited data recipient should be able to describe the purpose for each of these accounts. Further, these accounts should be treated in the same way as administrative accounts in regards to monitoring and logging practices.	**9.2.1** - A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	**8.1** - Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components. Assign all users a unique user name before allowing them to access system components or cardholder data. **8.5** - Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment.	**CC6.1** - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	2	1
		Password authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history, and password ageing.	Password authentication parameters should include the following as a minimum standard of requirements: **Password History:** > 12 **Password Age:** < 60 days **Password Length:** >8 **Complexity Requirements*:** Enabled **Storage:** Encrypted **Lockout Duration:** Until unlocked by admin, or other verification process such as asking various security questions. **Lockout Threshold:** <6 invalid attempts **Reset Account Lockout Counter:** >15 minutes *At least three of: Uppercase letters, lowercase letters, numerals, non-alphanumeric characters.	**9.4.3** - Password management systems shall be interactive and shall ensure quality passwords.	**8.2** - Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.	**CC6.1** - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	2	1

#	Control requirements	Minimum controls	Description of minimum controls	Additional guidance	ISO 27001	PCI DSS	Trust Services Criteria	PCI Prioritised Approach Milestone	SISS Suggested Priority
2	An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	**Encryption**	Encryption methods are utilised to secure CDR data at rest by encrypting fil systems, end-user devices, portable storage media and backup media. Cryptographic keys are securely stored, backed-up and retained. Appropriate user authentication controls (consistent with control objective 1) are in place for access to encryption solutions and cryptographic keys.	Encryption Solutions • All cryptographic keys used in a storage encryption solution are secured and managed properly to support the security of the solution. • Appropriate user authentication controls (in line with Control Objective 1 in this document) are in place for storage encryption solutions. Encryption Controls CDR data at rest on computer systems owned by an ADR and located within spaces, devices, and networks controlled by an ADR, are protected by one or more of the following mechanisms: • Disk or File System Encryption: Full disk encryption is implemented for external media and hard drives that are not fully encrypted but connect to encrypted USB devices, as thes are vulnerable to security breaches from the encrypted region to the unencrypted region. • Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure • Strong cryptography on authentication credentials and passwords to make these unreadable during transmission and storage on all information systems • File systems, disks, and tape drives in servers and Storage Area Network (SAN) environments are encrypted using industry standard encryption technology • Computer hard drives and other storage media that have been encrypted are reformatted to upon return for redistribution or disposal Portable devices, such as smart-phones and USB file storage, are not used for storage, processing, or transmission of any information related to CDR data environment. Encryption Key Management: • Appropriate user authentication controls (in line with Control Objective 1 in this document) are in place for encryption keys. • Appropriate back-up, retention and recoverability controls (in line with Control Objective 3) are in place for encryption keys.	**10.1.1** - A policy on the use of cryptographic controls for protection of information shall be developed and implemented. **10.1.2** - A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	**4.1** - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. internet, wireless technologies, cellular technologies General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission. **4.2** - Never send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	**CC6.1** - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. **CC6.7** - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	2	1
		Firewalls	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: (a) restrict all access from untrusted networks; and (b) denying all traffic aside from necessary protocols; and (c) restricting access to configuring firewalls, and review configurations on a regular basis.	All details provided in control wording. No additional guidance.	**13.1.1** - Networks shall be managed and controlled to protect information in systems and applications. **13.1.2** - Networks shall be managed and controlled to protect information in systems and applications.	**1.1** - Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; that document business justification and various technical settings for each implementation; that diagram all cardholder data flows across systems and networks; and stipulate a review of configuration rule sets at least every six months. **1.2** - Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment. **1.3** - Prohibit direct public access between the Internet and any system component in the cardholder data environment. **1.4** - Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment. **6.6** - Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerabilit assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**CC6.1** - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	1	1
		Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.	Acepted industry standards for hardening servers may include benchmarks and guidance provided by leading bodies such as the ACSC and CIS. Both of which are accepted as leading standards and are free to access. Reference links: https://www.cisecurity.org/cis-benchmarks/ https://nvd.nist.gov/ncp/repository	14.2.5 - Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	**2.2** - Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	**CC7.1** - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	3	2
		End-user devices	End-user devices, including bring-your-own-device (BYOD) systems, are hardened in accordance with accepted industry standards.	Acepted industry standards for hardening end-user devices may include benchmarks and guidance provided by leading bodies such as the ACSC and CIS. Both of which are accepted as leading standards and are free to access. Reference links: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf https://www.ncsc.gov.uk/collection/end-user-device-security	**6.2.1** - A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. **6.2.2** - A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	**1.4** - Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment. **12.3** - Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.	**CC3.2** - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. **CC6.1** - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. **CC6.7** - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	2	1
3	An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle.	**Data loss prevention**	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: (a) blocking access to unapproved cloud computing services; and (b) logging and monitoring the recipient, file size and frequency of outbound emails; and (c) email filtering and blocking methods that block emails with CDR data in text and attachments; and (d) blocking data write access to portable storage media.	All details provided in control wording. No additional guidance.		**A3.2.6 -** Implement mechanisms for detecting and preventing clear text PAN from leaving the CDE via an unauthorized channel, method, or process, including generation of audit logs and alerts.	**CC6.7** - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	1	1
		CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.	In general, CDR data should not be stored in non-production environments unless all controls are equivalent to those in in the production environment. Where an accredited data recipient must use CDR data in non-production environments, such as test or development environments, the accredited data recipient must ensure that the data is masked to ensure the ongoing confidentiality of the data.	**14.3.1** - Test data shall be selected carefully, protected and controlled.	**6.4** - Follow change control processes and procedures for all changes to system components. Ensure all relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes.	**CC8.1** - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	3	2
		Information asset lifecycle (as it relates to CDR data)	An accredited data recipient must document and implement processes that relate to the management of CDR data over its lifecycle, including an information classification and handling policy (which must address the confidentiality and sensitivity of CDR data) and processes relating to CDR data backup, retention, and, in accordance with rules 7.12 and 7.13, deletion and de-identification.	An accredited data recipient should give consideration to how CDR data will be managed over its lifecycle, particularly in regards to ensuring the security and confidentiality of CDR data and how data will be deleted or deidentified following withdrawal of consent. An accredited data recipient must then define and document policies and procedures for how this will be managed. The information lifecycle may be defined as moving through the following phases: 1) creation or collection; 2) storage, use, process and/or modification; and 3) deletion, de-identification or archiving. An accredited data recipient's policies should include all of the above mentioned phases as a minimum. Consideration should also be given to the creation of derived data from the initially collected CDR data.	**8.2.1** - Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. **8.2.2** - An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. **8.2.3** - Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. **8.3.2** - Media shall be disposed of securely when no longer required using formal procedures. **12.3.1** - Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy		**CC6.1** - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	1	1

#	Control requirements	Minimum controls	Description of minimum controls	Additional guidance	ISO 27001	PCI DSS	Trust Services Criteria	PCI Prioritised Approach Milestone	SISS Suggested Priority
4	An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	**Security patching**	A formal program is implemented for identifying, assessing the risk of and applying security patches to applications and operating systems as soon as practicable.	An accredited data recipient should have a defined patching cycle for systems within the CDR data environment. The patch cycle includes monitoring and identification of newly available patches, assessment and prioritisation, testing and application into the environment. Refer to https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches for a definition and examples of "extreme risk" vulnerabilities.	**12.6.1** - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	**6.2** - Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	**CC7.1** - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	3	2
		Secure coding	Changes to the accredited data recipient's systems (including its CDR data environment) are designed and developed consistent with industry accepted secure coding practices, and are appropriately tested prior to release into the production environment.	Acepted industry standards for secure coding may include benchmarks and guidance provided by leading bodies such as OWASP, which are accepted as leading standards and are free to access. Reference links: https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide	**14.2.1** - Rules for the development of software and systems shall be established and applied to developments within the organization.	**6.5** - Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines – including how sensitive data is handled in memory.		3	2
		Vulnerability Management	A formal vulnerability management program is designed and implemented, which includes regular vulnerability scanning and penetration testing on systems within the CDR data environment.	The vulnerability management program should complement the patching program defined above. The program should include formal processes for identification, tracking and remediation of vulnerabilities. Further, internal targets should be made taking into account metrics around proportion of vulnerabiltiies, their criticality and timeliness, e.g. '80% of High r vulnerabiltiies within 7 days of identification'.	**12.6.1** - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	**11.2** - Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff. **11.3** - Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls.	**CC7.1** - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	2	1
5	An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment.	**Anti-malware anti-virus**	Anti-virus and anti-malware solutions are implemented on endpoint devices and on servers to detect and remove malware from the CDR data environment and are updated on a regular basis. End-user systems are updated with the latest virus definitions when they connect to the network. Reports or dashboards highlighting compliance metrics are regularly generated and monitored, and non-compliant items are actioned as soon as practicable.	All details provided in control wording. No additional guidance.	**12.2.1** - Detection, prevention and recovery controls to protect againstmalware shall be implemented, combined with appropriate user awareness.	**5.1** - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software. **5.2** - Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7. **5.3** - Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	**CC6.8** - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	2	1
		Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.	All details provided in control wording. No additional guidance.		**1.2** - Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment. **6.6** - Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerability assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**CC6.8** - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	2	1
		Application whitelisting	Download of executables and installation of software on infrastructure and end-user devices (including on BYOD devices) is restricted to authorised software only.	All details provided in control wording. No additional guidance.	**12.5.1** - Procedures shall be implemented to control the installation of software on operational systems **12.6.2** - Rules governing the installation of software by users shall be established and implemented.		**CC6.8** - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	3	2
6	An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data.	**Security training and awareness**	All users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually.	Security and privacy training should include at a minimum: - personnel's responsibilities towards securing data and meeting their privacy obligations; - the organisation's expectations of personnel in interacting with systems and data within the CDR data environmentand and what is acceptable usage; - common security threats (e.g. email scams, malware, phishing, social engineering) and how to identify and address them; - physical security and clean desk requirements.	**7.2.2** - All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	**12.6 -** Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	**CC2.2** - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	6	3
		Acceptable use of technology	A policy relating to the CDR data environment is created, implemented, communicated and agreed to by all personnel prior to being able to access the CDR data environment. This policy sets out the responsibilities of these personnel in interacting with the CDR data environment and is regularly made aware to personnel.	An acceptable use of technology policy should include the obligations and requirements of personnel when interacting with systems or data within the CDR data environment in regards to security and privacy. These obligations should be agreed to by all personnel interacting with the CDR data environment (such as through an e-signature) and disciplinary action resulting from breach of the policy should be defined and enforced. Where possible, monitoring of compliance to this policy should be implemented, such as through web and email content filtering (see above).	**8.1.3** - Rules for the acceptable use of information and of assets associated with information and information processing facilities sha be identified, documented and implemented.	**12.3 -** Develop usage policies for critical technologies and define proper use of these technologies. **12.3.5** Acceptable uses of the technology	**CC1.1** - The entity demonstrates a commitment to integrity and ethical values. **CC1.5** - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	6	3
		Human resource security	Background checks are performed on all personnel prior to their interacting with the CDR data environment. These may include, but are not limited to, reference checks and police checks.	Background checks should be performed for all personnel interarcting with the CDR data environment. The extent of these checks are at the discretion of the organisation, but at a minimum should include police checks. The purpose of this is to help ensure the security and confidentiality of CDR data.	**7.1.1** - Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	**12.7 -** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.)	**CC1.4** - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	6	3

Appendix - Transaction Scopes

Scope Name	Scope ID	0 Public	1 Restricted Accrediation	2 Full Accrediation	Description
Basic Bank Account Data	bank:accounts.basic:read	No	Yes	Yes	This scope would allow for the third party to access basic information of the customer’s accounts. Includes simple account information including balance. Does not include account identifiers, product information or transaction data.
Detailed Bank Account Data	bank:accounts.detail:read	No	No	Yes	This scope would allow for the third party to access detailed information of the customer’s accounts. This scope is effectively additional authorisation to the Basic Bank Account Data scope. Granting this authorisation only makes sense if the Bank Account Data scope is also authorised. Includes basic account information plus account identifiers and product information. Does not include transaction data.
Bank Transaction Data	bank:transactions:read	No	Yes	Yes	This scope would allow the third party to access transaction data for accounts. This scope is effectively additional authorisation to the Basic Bank Account Data scope. Granting this authorisation only makes sense if the Basic Bank Account Data scope is also authorised. Includes all account transaction data.
Bank Payee Data	bank:payees:read	No	No	Yes	This scope allows access to payee information stored by the customer. Includes payee information such as billers, international beneficiaries and domestic payees.
Bank Regular Payments	bank:regular_payments:read	No	No	Yes	The scope would allow the third party to access regular payments. Includes Direct Debits and Scheduled Payments.
Basic Customer Data	common:customer.basic:read	No	Yes	Yes	The scope would allow the third party to access personally identifiable information about the customer. For retail customers this would be information about the customer themselves. For business customers it would imply the name of specific user but also information about the business. Includes name and occupation for individuals or name, business numbers and industry code for organisations
Detailed Customer Data	common:customer.detail:read	No	No	Yes	The scope would allow the third party to access more detailed information about the customer. Includes the data available with the Basic Customer Data scope plus contact details. Includes basic data plus phone, email and address information.
Public	NA	Yes	Yes	Yes	Openly accessible information. A customer would never need to grant this scope. This scope is included so that end points that can be called without requiring authorisation can be identified. Includes access to openly available information such as generic product information.
new Detailed Bank Transactic	bank:transactions.detailed:read	No	No	Yes	This is a new scope which splits the current Bank Transaction data into a basic level and a detailed level

Appendix - Transaction Accounts

Name	Type	Required	Restrictions	Basic (restricted accrediation)	Detailed (full accrediation)	Description
accountId	ASCIIString	mandatory	none	Yes	Yes	A unique ID of the account adhering to the standards for ID permanence
creationDate	DateString	optional	none	Yes	Yes	Date that the account was created (if known)
displayName	string	mandatory	none	No	Yes	The display name of the account as defined by the bank. This should not incorporate account numbers or PANs. If it does the values should be masked according to the rules of the MaskedAccountString common type.
nickname	string	optional	none	No	Yes	A customer supplied nick name for the account
openStatus	string	optional	none	Yes	Yes	Open or closed status for the account. If not present then OPEN is assumed
isOwned	Boolean	optional	none	No	Yes	Flag indicating that the customer associated with the authorisation is an owner of the account. Does not indicate sole ownership, however. If not present then 'true' is assumed
maskedNumber	MaskedAccountString	mandatory	none	Yes	Yes	A masked version of the account. Whether BSB/Account Number, Credit Card PAN or another number
productCategory	BankingProductCategory	mandatory	none	Yes	Yes	The category to which a product or account belongs. See here for more details
productName	string	mandatory	none	Yes	Yes	The unique identifier of the account as defined by the data holder (akin to model number for the account)

Name	Type	Required	Restrictions	Basic (restricted accrediation)	Detailed (full accrediation)	Description
accountId	ASCIIString	mandatory	none	yes	yes	A unique ID of the account adhering to the standards for ID permanence
currentBalance	AmountString	mandatory	none	yes	yes	The balance of the account at this time. Should align to the balance available via other channels such as Internet Banking. Assumed to be negative if the customer has money owing
availableBalance	AmountString	mandatory	none	no	yes	Balance representing the amount of funds available for transfer. Assumed to be zero or positive
creditLimit	AmountString	optional	none	no	yes	Object representing the maximum amount of credit that is available for this account. Assumed to be zero if absent
amortisedLimit	AmountString	optional	none	no	yes	Object representing the available limit amortised according to payment schedule. Assumed to be zero if absent
currency	CurrencyString	optional	none	yes	yes	The currency for the balance amounts. If absent assumed to be AUD
purses	[BankingBalancePurse]	optional	none	no	yes	Optional array of balances for the account in other currencies. Included to support accounts that support multi-currency purses such as Travel Cards

Appendix - Transactions

Name	Type	Required	Basic (restricted accrediation)	Detailed (full accrediation)	Description
accountId	ASCIIString	mandatory	Yes	Yes	ID of the account for which transactions are provided
transactionId	ASCIIString	conditional	Yes	Yes	A unique ID of the transaction adhering to the standards for ID permanence. This is mandatory (through hashing if necessary) unless there are specific and justifiable technical reasons why a transaction cannot be uniquely identified for a particular account type
isDetailAvailable	Boolean	mandatory	No	Yes	True if extended information is available using the transaction detail end point. False if extended data is not available
type	string	mandatory	Yes	Yes	The type of the transaction
status	string	mandatory	Yes	Yes	Status of the transaction whether pending or posted. Note that there is currently no provision in the standards to guarantee the ability to correlate a pending transaction with an associated posted transaction
description	string	mandatory	Yes	Yes	The transaction description as applied by the financial institution
postingDateTime	DateTimeString	conditional	Yes	Yes	The time the transaction was posted. This field is Mandatory if the transaction has status POSTED. This is the time that appears on a standard statement
valueDateTime	DateTimeString	optional	Yes	Yes	Date and time at which assets become available to the account owner in case of a credit entry, or cease to be available to the account owner in case of a debit transaction entry
executionDateTime	DateTimeString	optional	Yes	Yes	The time the transaction was executed by the originating customer, if available
amount	AmountString	mandatory	Yes	Yes	The value of the transaction. Negative values mean money was outgoing from the account
currency	CurrencyString	optional	Yes	Yes	The currency for the transaction amount. AUD assumed if not present
reference	string	mandatory	Yes	Yes	The reference for the transaction provided by the originating institution. Empty string if no data provided
merchantName	string	optional	No	Yes	Name of the merchant for an outgoing payment to a merchant
merchantCategoryCode	string	optional	No	Yes	The merchant category code (or MCC) for an outgoing payment to a merchant
billerCode	string	optional	No	Yes	BPAY Biller Code for the transaction (if available)
billerName	string	optional	No	Yes	Name of the BPAY biller for the transaction (if available)
crn	string	optional	No	Yes	BPAY CRN for the transaction (if available)
apcaNumber	string	optional	No	Yes	6 Digit APCA number for the initiating institution