SISS Data Services

SISS Data Services

Submission in response to Consumer Data Right (CDR) Consent Review

October 2023

SISS Data Services

For over 12 years, SISS Data Services (SDS) has provided secure bank data solutions to financial technology (FinTech) companies, especially accounting software platforms, and their small business customers.

Around 500,000 Australians have relied on SDS to securely deliver their banking data transactions into software platforms using direct feed arrangements with leading Australian banks and, more recently, through the Consumer Data Right (CDR) environment in which SDS is an Accredited Data Recipient (ADR).

SDS has never used screen-scraping and provides data only through bank-approved channels. As such, SDS is trusted by all of Australia's largest banks as well as leading accounting software platforms (including global giants Intuit QuickBooks and Sage) to provide high reliability, secure, permission-based bank data feeds for their mutual small business customers.

As Australia's leading independent provider of bank-approved data feeds to small businesses, SDS welcomes the opportunity to respond to the Screen Scraping discussion paper.

Overview

Consumers, including businesses and their Trusted Adviser, will rely on CDR data for a number of use cases, including to make financial decisions, lodge Tax Returns, claim GST and comply with their legal and statutory obligations. Historically, Consumers, business and their Advisers have relied upon physical bank statements or Closed Banking data feeds (Banks' own feeds), as it is data from the source of truth from the banks.

In its current state, the Consumer Data Right is still young and has some areas that require changes to mature and drive growth in the use of the ecosystem. We believe in the CDR regime and hope for it to improve and the forthcoming Business Disclosure use consent will assist with this. We thank the Treasury and associated regulators for undertaking this consent review; our feedback and answers to the questions proposed in the review document are documented in the following pages.

What screen scraping practices are you aware of or involved in? a) What is the scope and purpose of the data that is captured? Is the data that is captured only banking data, or does it include data from other sectors? b) What steps do consumers, screen scraping service providers and businesses using screen scraping take in the screen scraping process? What information is provided to consumers through the process? c) When is the consumer's data accessed as a one-off, and when is longer-term or ongoing access obtained? Where ongoing access is in place, how are consumers made aware of this and can they cancel access at a later point? d) Do you use screen scraping for purposes other than data collection (for example to undertake actions on behalf of a customer)?
We currently do not use screen scraping practices. We have considered this technology on several occasions as it could meet the needs of our clients, however, we decided to use something other than screen scraping. We instead elected to utilise direct contractual relationships with the banks. The direct method of data collection met our quality, security and reliability requirements. A significant factor in electing to use direct collection was consumer expectations; the idea of collecting and storing their login credentials was out of step with how data 'should' be collected. We (and our clients) also had issues with asking consumers to wilfully breach the banks' internet banking T&Cs, along with any consequences that may entail. Our current experience suggests that many consumers must be made aware of how data is acquired. Screen scraping is often presented in a way they proceed and unwittingly believe they are using a sanctioned (bank-approved) data collection method.
Are there any other risks to consumers from sharing their login details through screen scraping?
We aren't aware of any breaches or issues.
2 Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?
No, other than our concerns that banks may reject (legitimate) claims of a consumers suffer a lose data if they have previously used a screen scraping service.
3 Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?
No
4 Could you provide any examples of actions your organisation takes to prevent or block screen scraping (if you hold the consumer's data, such as a bank), or when your company's use of screen scraping has been blocked (if you provide screen scraping services or you partner with a screen scraper to provide your services), and why?
We don't screen scrap. Our method of direct bank connection for 11 years has not suffered a single significant outage or case of data being blocked. Have we had minor delays and errors? Yes, but these are usually sub two hours, and we have had an extremely reliable data delivery.
5 Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?
n/a
6 Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?
n/a
7 Are there any other international developments that should be considered?
Based on Australian CDR history, the obvious consideration is the UK Open Banking reforms. However, we note the increased international interest in Open Banking & CDR-like regimes, for example, recent moves in countries like New Zealand and the very recent announcements in the USA.
8. What are your views on the comparability of screen scraping and the CDR? a) Can you provide examples of data that is being accessed through screen scraping

that cannot currently be accessed using the CDR or vice versa?
b) Are there particular restrictions related to data use and disclosure under the CDR that influence choices to continue using screen scraping, or vice versa?
c) Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?
d) Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?

A-
While we don't specifically use Screen Scraping, we do work with some parties that do. Data is close, but there are some differences;

1) Bank balances – screen scraping has the ability to see a bank account as a proper ledger with a running balance. CDR does not offer this; to date, we have found some Data Holders to provide very poor balances via CDR. That is, the balance reported via CDR does not represent or match the balance shown on their digital platforms. Having a running balance to reconcile allows us to ensure completeness of data; at present, this for some data holders is not possible for a number of reasons.
2) Account discoverability: screen scrapping technology allows a data recipient to discover all the bank accounts a consumer may have. This doesn't mean a recipient collects data for all accounts, as the consumer is able to select which accounts they wish to share, but it does allow a data recipient to validate the consumer selection and monitor the list of accounts. A practical benefit of this is that a recipient is able to detect if a new account is opened and then prompt the consumer to include or exclude it from their share.
3) The current quality of transaction descriptions in CDR does not match the experience consumers have on the bank's digital platform(s). This is a data quality issue requiring enforcement action. However, screen scraping is currently able to obtain more 'complete' transaction descriptions.

D-
One significant issue we have with CDR at present is the separation of the transaction & transaction detail calls, as a number of Data Holders do not include transaction 'messages' and references within the transaction call. This requires an ADR to make transaction detail calls to obtain a message or reference a consumer includes in an Osko/NPP transaction. Per the current specifications, a transaction detail call can only be made for a single transaction. This restriction is problematic if a consumer or their customers transact via NPP/Osko as an ADR may need to make so many calls that they reach limits and become throttled. A simple solution would be a bulk transaction detail call, allowing an ADR to make a single call and reduce the load on a DH.

9. The Statutory Review recommended that screen scraping should be banned in the near future in sectors where the CDR is a viable alternative.
   a) How should the Government determine if the CDR is a viable alternative?

CDR has the potential to be far better than screen scraping and even the current direct contractual relationships we have with Banks.

There have been some recent reviews of the consent process for ADRs. This review has been positive but does need to be extended to the Data Holder side of the consent journey, as implementations across the DHs are varied and inconsistent and could be simplified.

To date, the CDR system has been very individual consumer-focused; however, in our experience, more 'business consumer' focused user cases exist. Issues like the nomination of secondary users have been a blocker. We cannot understate the impact of this; a number of beneficiaries of CDR data have not engaged with CDR due to the issues around business consumers having a complicated journey to give consent to an ADR.

Account discovery or disclosure of available accounts to an ADR. By no means do we suggest that a DH be required to disclose data about accounts the consumer has not given explicit consent to; however, screen scraping does provide the benefit of providing the entire list of available accounts. The feedback we have from customers

Data corrections and/or updates. There is a requirement for DHs to correct data. However, the requirements to update ADRs are not as well defined, and there was a defined process. This could be a significant improvement over existing data collection methods. Branding, at present, the “CDR” brand, is not widely known by the average consumer. The current website(s) are great, but as the ecosystem matures across more sectors, a public awareness campaign would be beneficial. We note while the CDR brand is not well known, the term ‘open banking’ is somewhat better known. However, this will change as more sectors are brought into CDR. Completeness of Data Holders: the current requirements have dragged many but not all the data holders into the CDR regime. We are concerned that some data holders will not be compelled to share data because they have arranged their business in a way to bypass (by accident or design) the CDR requirements. We feel this will affect non-bank lending more than the current sectors. However, there are already data holders who offer ‘transaction’ or ‘banking’ like products but are not ADIs, therefore outside of the scope of CDR. We are unsure of the exact nature of compelling these data holders into the CDR framework, but we already have consumers questioning the viability of the CDR ecosystem if “Company A” is not compelled to share data. Unfortunately, some (but not all) of these fringe data holders are available via screen scraping.
b) What are your views on a ban on screen scraping where the CDR is a viable alternative?
We feel that screen scraping only exists because there is no alternative. It was created and adopted because there was a business case for requiring & using consumer data. Therefore, as a sector comes online for CDR, screen scraping should have a sunset after 12 months.
c) What timeframe would be required for an industry transition away from screen scraping and why?
We believe the transition should happen sooner rather than later and would support a ban from 1 Feb 2025