Skript

Submission to Treasury

Consumer Data Right discussion paper: screen scraping – policy and regulatory implications

Submission by:
Skript Pty Ltd

25 October 2023

Skript (ABN 23 648 590 845)
Level 8, 124 Walker Street
North Sydney, NSW 2060

Introduction

Skript welcomes the opportunity to respond to the screen scraping discussion paper through this consultation by Treasury.

An introduction to Skript

Skript (we) was founded on the vision that the future will be about taking banking services to customers rather than making them go directly to a bank. We create solutions that connect businesses to the world of the Consumer Data Right (CDR) to enable the services of this future.

It has become evident to us that consumers, both individuals and businesses alike, are seeking CDR as an alternative to existing data sharing mechanisms owing to its clear benefits in terms of data security, transparency, and control. Skript is deeply committed to driving systemic adoption of the CDR to bring these benefits to consumers.

A summary of this submission

Skript is an unrestricted accredited data recipient (ADR) with the CDR and is not directly involved with any screen scraping practices. We see the clear value CDR offers consumers and believe it is the future of open data in Australia.

Skript is supportive of banning screen scraping and moving to the CDR given the benefits this will bring to consumers. However, we see five key areas that require attention for the CDR to be a truly viable alternative for the current usage of screen scraping.

1. **Consent experience and consumer accessibility:** Recent consultations on operational enhancements and the CDR consent process have proposed immense improvements to the CDR. A more streamlined consent process and improved accessibility of the CDR, in particular for non-individual consumers, will significantly increase the CDR's viability.
2. **Limitations on the use of CDR data:** CDR data, and any data directly or indirectly derived from it, is subject to stringent privacy protections and restrictions. While Skript acknowledges the value of these protections, they do present practical challenges for a number of use cases. For example, the rules around data deletion or de-identification and the limitations around derived data mean CDR is not a viable option for many use cases. These protections are not applied to data collected in any other way, even when collected directly from a consumer.
3. **Product and industry coverage:** The CDR must encompass all publicly offered products in the designated industries to replace the data coverage that screen scraping offers. Skript has observed at least one instance where a data holder has excluded their digital channel targeted towards corporate customers from the CDR, irrespective of the underlying product or consumer eligibility. Exclusions of this nature will present issues if

consumers currently relying on screen scraping are moved to the CDR. In terms of industry coverage, Skript strongly recommends that the expansion of the CDR prioritises Open Finance given existing solutions leveraging screen scraping primarily operate in this space.

4. **Regulatory enforcement:** Adherence to the CDR Rules, standards and CX guidelines must be enforced if the CDR is to be a truly viable alternative to screen scraping. This applies to data holders and recipients alike. Issues raised on data availability, quality or the availability of other areas of the CDR must be dealt with as a priority from all parties to resolve the issue as best and as quickly as possible for consumers. Consumers will pay the price for a lack of serious consequences to CDR participants missing their obligations.
5. **Data quality:** The quality of CDR data is paramount in ensuring the CDR's viability when screen scraping is banned. CDR data should at least mirror data available through a data holder's online platform. We have seen instances of CDR data being handled differently to data in online platforms, for example through over-masking transaction descriptions only for CDR data.

If the above challenges with the CDR are addressed, Skript is confident that consumers will benefit from more reliable, transparent and secure services. None of these areas require significant implementation effort, and can be addressed concurrently while businesses prepare for a migration to CDR.

This submission contains our responses to the questions in the discussion paper that were relevant to us as an ADR with no direct involvement in screen scraping.

1. What screen scraping practices are you aware of or involved in?

1a) 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?

While Skript is not directly involved in screen scraping, we are aware of the varied scope and purpose of data captured. Screen scraping allows fintechs to capture not only banking data but extends to other sectors, such as non-bank lending, wealth, superannuation, as well as the public sector (such as the Australian Tax Office). The majority of use cases supported by screen scraping today seem to be related to a consumer's finances in some form.

1b) 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?

One of the challenges with screen scraping is the lack of standardisation and regulation. As such, it is not surprising that we have observed large variances in UX, functionality and technical processes across different providers.

Some providers have introduced a digital consent process somewhat comparable to CDR, albeit this will always exclude the handoff to a data holder to authenticate and authorise the data sharing arrangement. However, the presence and quality of consent processes vary among providers in terms of thoroughness and transparency for consumers.

1c) 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?

We are aware that consumers are not consistently and prominently informed whether their data will be accessed as a one-off or longer-term. Consumers are also not empowered to withdraw their 'consent' in a consistent manner other than asking their service provider to terminate the data collection, use and disclosure. There is no standardised mechanism for a consumer to withdraw the 'consent' from the data holder side other than by changing their password, which may not be intuitively apparent to them.

Once again, the lack of standardisation and regulation means there will be varying positions on consumer transparency and control across screen scraping providers.

2. What are the risks of screen scraping?

2a) Are there any other risks to consumers from sharing their login details through screen scraping?

Skript agrees with the risks identified in the discussion paper. In addition, we see the following risks:

- **Lack of transparency**: Consumers are not always informed on how screen scraping operates, and the risks involved. There are limited requirements for providers to disclose how a consumer's data will be collected, used and disclosed, and which parties are involved. This may lead to consumers being unaware of the risks highlighted in the discussion paper when agreeing to the data sharing. Skript has also encountered on numerous occasions that consumers as well as trusted adviser professionals have confused screen scraping for the CDR where solutions don't readily identify themselves as screen scraping solutions.
- **Lack of control**: Consumers have no standardised way of controlling how their data is used, and by whom. There is no way of withdrawing a screen scraping 'consent' from a data holder's platform without changing login passwords, which may not be intuitive for consumers.

Skript is aware that some screen scraping providers have made concerted efforts to improve the transparency and control they offer consumers. However, these risks apply broadly to an industry that has little standardisation and regulation.

3. The Consumer Data Right

3a) What are your views on the comparability of screen scraping and the CDR?

Skript considers that the CDR offers consumers a clear benefit over screen scraping in terms of transparency, control, security and protections in relation their data. Therefore, we are supportive of a ban on screen scraping in favour of more secure data sharing mechanisms such as the CDR.

However, we see five key areas that require attention for the CDR to be a truly viable alternative for the current usage of screen scraping.

1. **Consent experience and consumer accessibility**

While the CDR offers superior consumer protections over screen scraping, it does introduce more friction to consumers. The CDR consent process currently involves anywhere upwards of

6 screens a consumer needs to click through, and most of these include a lot of information and require express action from a consumer. In contrast, screen scraping is able to offer a much more streamlined experience due to the lack of regulation and the absence of the handoff to data holders to authenticate and receive authorisation from a consumer. While there is value in a certain level of positive friction in the CDR process, by way of increased transparency and security, adoption will be hindered if consumers find this process too difficult. Simplifying the consent process will significantly increase the CDR's viability when screen scraping is banned.

Furthermore, we have observed that non-individual consumers are facing unreasonable friction when attempting to utilise the CDR. The processes implemented by data holders for nominated representatives to be appointed, which often involve wet-ink signature forms that need to be handed in to a branch, have proven to be insufficient. We have observed instances of business consumers being redirected to multiple departments, waiting months for responses, and in some instances being turned away altogether when attempting to access the CDR. Some data holders have even implemented a prerequisite step of 'activating' CDR for a non-individual consumer before a nominated representative can be appointed. Business consumers represent a large proportion of Australian consumers who can benefit from, and substantially drive the adoption of, the CDR. Many of these businesses are currently relying on screen scraping to connect their bank accounts with other systems and will require CDR to be more accessible so as not to disrupt their operations.

Recent consultations on operational enhancements and a consent review have directly addressed both of these areas and have been very welcomed by Skript. Based on the proposed amendments contained in those design papers, we are confident that the CDR is headed in the right direction to resolve these challenges.

2. Limitations on the use of CDR data

CDR data, and any data directly or indirectly derived from it, is subject to stringent privacy protections and restrictions. While Skript acknowledges the value of these protections, they do present a number of practical challenges for businesses looking to adopt the CDR.

Requirement to delete or de-identify CDR data when a consent expires

Consider a payroll provider that facilitates the employee onboarding process for businesses. As part of this process, the new employee must nominate a bank account in which they wish to receive their remuneration payments. If the payroll provider wishes to utilise CDR to collect the employee's bank account details, they must delete these details at the end of the consent period. In this case, given the employee is an individual, the maximum consent period is 12

months. Given it would be unreasonable to expect employees to complete an annual bank account selection process, the CDR does not offer a viable option for the collection of these details.

Services such as online investment applications could also benefit from the CDR as a way of collecting and storing validated bank account details. This would be particularly valuable in mitigating the risk of fraudulent withdrawals. However, these use cases face the same impracticality and therefore limited viability of the CDR.

Limitations on derived CDR data

Consider a consumer wishing to initiate a payment that is informed by CDR data. For example, a consumer may wish to transfer a roundup of each transaction they incur on their transaction account to their savings account. Given the limitations on the usage and disclosure of derived CDR data, in this case in the form of the roundup value of each transaction disclosed to a payment provider, the CDR offers significantly less viability than data obtained from other mechanisms such as screen scraping, or even obtained directly from the consumer.

Maximum consent duration

Recent changes permitting business consumers to grant use and disclosure consents for a period of up to 7 years have greatly improved the viability of the CDR for business use. However, business consumers still need to grant a new consent at least every 12 months given collection consents cannot extend past this period. Many business consumers have provided feedback to us that this is inconsistent and impractical, and limits the operational viability of the CDR. We strongly recommend extending the maximum duration of collection consents for business consumers to 7 years.

Skript firmly believes that the benefits of this change would far outweigh any potential risks. Business consumers would continue to receive regular notifications about their data sharing arrangements and maintain the flexibility to withdraw their consent at any time. Online consumer dashboards offer businesses centralised transparency, ensuring they remain constantly aware of active data sharing arrangements. Business data also typically carries lower risks than data relating to an individual, as demonstrated by recent changes allowing business consumer CDR data to be shared with any identified persons. Considering these factors, Skript strongly advocates extending the maximum period of collection consents for business consumers to 7 years, in line with the parameters for use and disclosure consents.

Definition of service data

Although it was discussed in the recent consultation on CDR operational enhancements, it's worth noting that if all data received by a CDR representative or accredited data recipient must be handled as 'service data' or fully protected CDR data, many more use cases will be excluded from the CDR. Skript recommended under that consultation that CDR data should be handled in line with the relevant consent received from the consumer, rather than the accreditation status of the entity, or which ADR disclosed the data.

3. Product and industry coverage

The CDR must encompass all publicly offered products in the designated industries in order to replace the data coverage that screen scraping offers. Skript has observed at least one instance where a data holder has excluded their digital channel targeted towards corporate customers from the CDR, irrespective of the underlying product or consumer eligibility. More broadly, Skript has encountered data holders stating to us, as well as to their consumers directly, that corporate or institutional level customers are out of scope for the CDR. This statement is not only contradictory to the CDR Rules but also undermines the value that the CDR promises business consumers. Businesses of any size can benefit from the CDR, but we have observed a particular gap in secure solutions for small to medium enterprises (SMEs) as well as smaller corporate customers to automate their data feeds. The scope of the CDR should be clear, and all publicly offered products should be accessible.

The other aspect of data coverage that screen scraping currently offers over the CDR is access to industries other than banking and energy. The large majority of services supported by screen scraping are related to a consumer's finances. As such, Skript recommends that the expansion of the CDR prioritises Open Finance over other industries such as telecommunications. This is indicative of where the market has found traction to date and will allow the CDR to maximise its adoption. It will also allow screen scraping to be phased out as these additional industries are designated into the CDR.

4. Regulatory enforcement

Adherence to the CDR Rules, standards and CX guidelines must be enforced if the CDR is to be a truly viable alternative to screen scraping. This applies to data holders and recipients alike.

While significant effort from industry and policy writers is directed towards the improvement of the CDR, this holds less weight if there is a lack of serious consequences for delaying or compromising compliance. Issues raised on data availability, quality, or the availability of other areas of the CDR must be dealt with as a priority from all parties to resolve the issue as best and as quickly as possible for consumers.

Consumers will be the ones to suffer if CDR compliance is not seriously enforced.

5. **Data quality**

The quality of CDR data is paramount in ensuring the CDR's viability when screen scraping is banned. While we have observed anecdotal feedback that CDR data is of higher quality than screen scraped data in some areas, improving and maintaining CDR data quality must be a consistent priority. CDR data should at least mirror data available through a data holder's online platform. We have seen instances of CDR data being handled differently to data in online platforms, for example through over-masking transaction descriptions only for CDR data.

In addition, the language used in the data standards describing certain fields as “optional” presents issues. While the intent behind this is that data holders should make that field available via CDR if it is available in other channels, it is sometimes interpreted that fields are truly optional.

3b) The Statutory Review recommended that screen scraping should be banned in the near future in sectors where the CDR is a viable alternative.

3b.1) How should the Government determine if the CDR is a viable alternative?

Skript firmly believes that the CDR is on the brink of becoming a truly viable alternative to screen scraping. In addition to the above criteria to assess its viability, we encourage the industry to undergo an exercise to estimate the volumes of data sharing arrangements that would migrate to the CDR. This could inform an assessment of the current non-functional requirements to ensure a successful migration.

3b.2) What are your views on a ban on screen scraping where the CDR is a viable alternative?

Skript is supportive of a ban on screen scraping where more secure data sharing methods such as the CDR offer viable alternatives.

3b.3) What timeframe would be required for an industry transition away from screen scraping and why?

Sufficient time should be allocated for existing service providers to migrate to the CDR, and to address the challenges currently experienced in the CDR. The foundations are already there, and none of these challenges require significant implementation effort on data holders or recipients, such as by introducing new industries or data types. Improvements to the CDR can also happen concurrently while businesses prepare for a migration to CDR. Skript considers that a transition should not reasonably take more than 18 months.