

Consumer Data Right Policy and Engagement Branch
Market Conduct and Digital Division
The Treasury
Langton Crescent
Parkes ACT 2600
Submitted via email to: data@treasury.gov.au

25 October 2023

Dear Sir/Madam,

Beforepay Group Limited (**Beforepay**) welcomes the opportunity to respond to the Treasury discussion paper on Screen scraping - policy and regulatory implications (**Paper**).

In this submission, we provide our views on the usability of the Consumer Data Right (**CDR**) versus screen scraping and the potential impact that a screen scraping ban would have on consumers and businesses in Australia.

About us

Beforepay was founded in 2019 as a mission-driven organisation to support working Australians. As part of this mission, we provide ethical loans and financial management tools to our consumers. We have over 1 million registered consumers across Australia.

Our short-term advance products aim to empower consumers to manage short-term financial challenges while avoiding predatory lending and avoiding the risk of long-term indebtedness.

We offer eligible consumers an advance of up to \$2,000 (average \$360) of their pay or tax refund, on-demand, for a 5% fixed transaction fee, with no interest or late fees. Alongside our pay advance and tax advance products, we also provide a bespoke budgeting tool, real-time spending insights and articles within our mobile app to promote good financial habits, further supporting responsible money management.

As part of providing our short-term advance products, we ask the consumer to sync their bank account to our system so that we can assess their creditworthiness. With consent from the consumer, we obtain access to a consumer's banking data using either screen scraping and the CDR, depending on the consumer's bank, and are therefore in a position to provide feedback on our experiences based on a direct comparison between the two.

Executive Summary

We are supportive of the CDR and are keen to use it as it is intended to operate. However, data holders need to take substantive actions both to improve CDR data quality and to make the regime more usable and fit for purpose.

Data provided under the CDR is often different from and of a lower quality than, data provided directly to consumers. Inaccurate data can lead to unfavourable consumer outcomes, such as inaccurate risk assessments, lending limits not appropriately sized for the consumer's financial situation, mistaken eligibility assessments, and an uneven playing field for new entrants.

In addition, the current consent flows discourage the use of the CDR by being too complex for an average consumer. We see this in the increased drop-off rates with the CDR. Based on our internal calculations, when enrolling in the Beforepay product, consumers are 5.7 times more likely to abandon the CDR flow than a screen scraping flow. Observed reasons for this difference include unnecessarily complex consumer experiences, and imbalanced warnings and representations of risks associated with the use of the CDR.

We believe that the CDR will be a viable alternative to screen scraping only when:

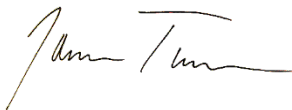
- CDR data is of the same quality as data presented to the consumer, such that:
 - CDR data contains the same information as the consumer is able to obtain directly from the bank, at the same level of quality;
 - consumers are not experiencing poor outcomes as a result of data recipients receiving poor-quality data;
 - data holders do not have a competitive advantage in cross-selling proprietary products to their consumers; and
- CDR consent throughput matches that of screen scraping throughput.

Until these thresholds are met, any decision to restrict screen scraping will reduce the ability of consumers to share their data. It will also reduce competition and slow the rate of innovation.

We set out below our detailed responses to the queries in the Paper in Attachment 1.

Thank you for the opportunity to contribute to this consultation. Should you wish to discuss our submission or require additional information, please do not hesitate to contact me.

Yours sincerely,



Jamie Twiss
Chief Executive Officer

Attachment 1 – Detailed response to the queries in the Paper

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

We primarily use screen scraping for data collection to facilitate and/or improve our services (including KYC checks, assigning appropriate borrowing limits, budgeting services, and providing pay and tax refund advances).

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?

The type of data that we capture is limited to banking data, and our access to this data is read-only.

For each consumer, the scope is limited to transactional information within the accounts that a consumer has with a bank. The data excludes any upcoming or scheduled payments within the account.

We use the data for the purposes of:

- to confirm that a consumer meets our eligibility criteria for our products, as set out in our Target Market Determination;
- to assess a consumer's creditworthiness to ensure that the product is not unsuitable for the individual;
- to determine a more accurate and comprehensive view of a consumer's borrowing limit by assessing items (a) and (b) above;
- to assist consumers with budgeting their personal finances by categorising their income and expenses, which is then displayed in our app for their use; and
- to support transaction monitoring and compliance with the AML/CTF Act.

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?

When a consumer creates an account with us, they must agree to our Terms of Service and Privacy Policy which lay out how their data might be used.

After this step, a consumer is required to verify their income in order to access our product. To do that, we ask them if they will allow us to sync their bank account with their Beforepay account, which allows us to assess their eligibility for the product and their creditworthiness.

If a consumer wishes to sync their bank account with us, we inform them that by doing so:

- Beforepay will have read-only access to their transactions;
- that Beforepay cannot make any changes to their bank account; and
- the information we receive as part of the bank syncing process is encrypted using bank-level security protocols.

A consumer can decline to connect their bank account, at which stage their application ceases.

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?

Our product is designed to be used periodically, with consumers drawing down a small advance when required and then fully repaying it. In addition, we provide free budgeting tools to all synced consumers. With prior consumer consent, we obtain ongoing access to their banking transactions, to provide up-to-date information in the budgeting tool and to pre-calculate eligibility and limits for returning consumers.

A consumer can cancel our access to their data at any point in time by contacting us to disconnect their synced bank accounts. Additionally, if a consumer changes their banking credentials (such as their password) our access to their data will also be automatically cancelled. We destroy or de-identify a consumer's information if they ask us to do so in a manner that is consistent with our privacy policy and the relevant legal and regulatory requirements.

If a consumer disconnects their bank account, and later wishes for our access to be reestablished, or if they wish to sync a different bank, the consumer will need to undertake the syncing process, including consent, afresh.

d) Do you use screen scraping for purposes other than data collection (for example to undertake actions on behalf of a customer)?

We primarily use screen scraping for data collection to facilitate and/or improve our services.

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

We are not aware of any other risks to consumers from sharing their login details through screen scraping.

A consumer's login details are not shared with us nor are they visible to us at any point as part of the screen scraping process. When consumers enter their login details on the screen presented to them, the details are shared directly with our third-party data provider, which then enables the syncing of the consumer's bank account to assess their eligibility for our product. We neither hold nor have access to the consumer's login details.

We take the privacy of our consumers very seriously. We perform risk assessments when considering new suppliers and only onboard third-party suppliers with sound security controls and industry-based certifications. We regularly monitor our third-party suppliers in respect of their information security practices, to obtain assurance that consumer login information is protected on their end.

3. Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?

We are not aware of any specific instances or cases of any loss or security breach to a consumer as a result of a consumer sharing their login details through screen scraping.

We apply the same high information security standards to protect all consumer data that we hold, whether it was acquired by screen scraping or the CDR.

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 do not hold or provide data for other organisations to screen scrape.

We have had instances where our access to screen scraping has been turned off due to:

- a data holder's decision to block screen scraping through the implementation of technical controls; and/or
- CDR data holders altering their information security protocols which then required changes to our service provider's operations.

We are very supportive of increased security protocols and take the privacy of our consumers seriously. We believe that as long as the CDR continues to suffer from poor usability and quality, screen scraping improves data security overall, as it reduces the likelihood of consumers sharing data through less secure means such as emailing financial information. We also note that we are unaware of any privacy or security incidents caused by screen scraping.

We are supportive of additional steps to further enhance the security of screen scraping. One such step could be whitelisting dedicated IP addresses for verified third parties to securely access data, which reduces the potential risk of bad actors. This would improve security across the system.

5. *Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?*

We obtain screen scraping services via a third party. With sound third-party onboarding practices in place, we are aware of and regularly perform monitoring over the security measures of our third party to ensure that consumer data is protected. Some measures taken by our third-party provider include:

- the third party provider's physical environment is hosted and managed in data centres that are certified for international standards such as ISO 270001, and progress is being made towards SOC 2 compliance;
- formal risk management framework to identify, mitigate, and address risks effectively;
- regular penetration testing of systems;
- data encrypted at rest and in transit using industry-standard techniques; and
- mandated security compliance processes for all consumers to ensure there are adequate controls and a positive security culture.

6. Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?

We are not aware of any proposed reforms or legal frameworks that relate to the use of screen scraping.

However, we believe that a ban on screen scraping without first resolving the data quality issues in the CDR will increase the difficulty of compliance with the obligations under existing legal frameworks, such as:

- **National Consumer Credit Protection Act 2009 (Cth)** - particularly for the purposes of responsible lending;
- **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)** - for the purposes of transaction monitoring and suspicious matter reporting.

7. Are there any other international developments that should be considered?

We are not aware of any other international developments that should be considered for the purposes of this consultation.

8. What are your views on the comparability of screen scraping and the CDR?

1. Data quality

Data quality obtained via the CDR is often incomplete and inaccurate when compared to screen scraping. Some specific and recurring examples include:

- inaccurate transaction descriptions containing random special characters; and
- important information being stripped out of descriptions before being provided to data recipients.

As a general rule, we are aware that banks take measures to clean and process the data they provide directly to consumers so that it is as comprehensive and accurate as possible. It appears that many banks do not provide the same data through the CDR, but instead provide lower-quality data pulled from raw tables without the same quality control and processing. Some also modify the transaction description limiting the data quality.

2. Consumer experience

The current consumer experience and consent flow of the CDR can be confusing and require more steps and time to complete than the screen scraping process.

The CDR consent process varies by data holder. It usually has four to six screens that a consumer must read through to connect their account, compared to one to two screens for screen scraping. In addition, the messaging in the consent flow generally provides little information about security measures taken by data recipients, and generally fails to indicate that declining to share data or limiting the information shared will likely affect the availability of products. This is evidenced by the consumer drop-off rates that Beforepay observes under the CDR, approximately 5.7x the drop-off rate in screen scraping, based on our internal calculations.

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?

Some examples of data that can be accessed through screen scraping that cannot currently be accessed using the CDR are:

- entire bank statements can be accessed using screen scraping, removing the need for consumers to provide this information to service providers;
- fields such as category information are automatically collected through screen scraping, whereas these fields are optional under the CDR; and
- CDR allows for some information to be masked, and the provision of such information tends to vary between institutions.

In addition, because the quality issues in CDR data vary by bank, algorithms and risk models used by data recipients struggle to use the inconsistent data, whereas screen scraping data is significantly more uniform. It is much easier to train models on consistent data.

These limitations prevent consumers from sharing their data fully under the CDR. This could deliver unfavourable consumer outcomes such as inaccurate determinations of consumer eligibility or suitability, as well as credit decisions outside affordability. It may also encourage consumers to share their data in less secure ways, such as providing bank statements and payslips that contain additional sensitive information.

These limitations also reduce the ability of data recipients to compete with incumbents.

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?

There are no statutory restrictions in the CDR that influence our decision to continue using screen scraping.

Our choice to continue using screen scraping where possible, instead of the CDR, is the result of the lower data quality and high drop-off rates observed with the CDR. We look forward to moving to the CDR as soon as it is operating at an acceptable level of quality.

c) Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?

While we have not explored these risks in detail, we believe that there could be two potential regulatory frameworks that may affect the viability of the CDR as an alternative to screen scraping.

- ***National Consumer Credit Protection Act (2009) (Cth):*** Inaccurate or inconsistent data may make it more difficult to assess credit risk and could impact responsible lending practices.
- ***Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth):*** Miscategorised transactions could make it more difficult to identify and report potential

suspicious matters or illegal activity to the regulator, which is a key compliance requirement for providers of designated services.

d) Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?

Our suggestions are as follows:

- a clear and consistently enforced requirement that data holders must provide the same transaction detail, descriptions, and categorisation as they provide to their own customers, and that data holders must not strip information out of merchant transaction descriptions before passing it along to data recipients;
- Simplification of the CDR consent flow, including a reduction of the number of screens required to complete;
- Consistent monitoring and publication of data around uptime and performance of CDR data holders.

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?

We believe that the CDR can be considered a viable alternative to screen scraping only when:

- CDR data is of the same quality as data presented to the consumer, including:
 - CDR data contains the same information that consumers receive directly from their banks, with the same level of detail and quality;
 - Consumers are not experiencing poor outcomes as a result of data recipients receiving poor-quality data;
 - CDR data is of a quality (in terms of accuracy, completeness, timeliness, consistency, availability and fitness for use) that enables data recipients to appropriately manage their own data risk, including their own regulatory obligations; and
- CDR consent throughput matches that of screen scraping throughput.

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

As it currently stands, the CDR is not a viable alternative to screen scraping, for the reasons discussed elsewhere in our submission.

As noted above, we are supportive of a transition from screen scraping to the CDR only when:

- CDR data is of the same quality as data presented to the consumer, and it contains as much information as the consumer is able to obtain directly otherwise from the bank;
- consumers are not experiencing poor outcomes as a result of data recipients receiving poor-quality data; and
- CDR consent throughput matches that of screen scraping throughput.

When these standards are reached, we believe screen scraping will likely fall away without requiring a ban.

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

This is a question that can only be answered by the data holders. The transition can only begin when data holders are providing acceptable quality data and empowering consumers who would like to share their data.

A forced transition to the CDR from screen scraping without addressing its current issues will result in:

- consumers experiencing greater difficulty in sharing their data;
- a reduction in competition in the financial services industry; and
- a slowdown in innovation.