

25 October 2023

Consumer Data Right Policy and Engagement Branch  
Market Conduct and Digital Division  
The Treasury  
Langton Crescent  
PARKES ACT 2600

By email: [data@treasury.gov.au](mailto:data@treasury.gov.au)

Dear Sir/Madam,

**Re: Screen Scraping – Policy and Regulatory Implications – Consultation**

Credit Corp welcomes the opportunity to provide feedback on Treasury’s Screen Scraping – Policy and Regulatory Implications Discussion Paper.

Credit Corp considers that screen scraping continues to provide an effective and broadly safe alternative, whilst CDR within Australia remains in its very early stages. It supports competition in the finance market with its accessibility to smaller and emerging providers.

As set out below, we consider that screen scraping should remain available, with any phasing out to be a natural consequence of open banking making the practice redundant by facilitating a more efficient data transfer mechanism.

Credit Corp

Credit Corp is an online lender delivering responsible loans with competitive fees and interest rates. We service, among others, consumers with limited borrowing alternatives. Through our Wallet Wizard Smart Loan, we deliver loans that are up to 76% cheaper than alternative borrowing options.<sup>1</sup> At the end of FY23, Credit Corp’s loan book was approximately \$358 million, servicing over 400, 000 consumers.

Screen Scraping - Benefits

Credit Corp relies on the availability of screen scraping to support its obligations under the responsible lending laws. Screen scraping is vital in supporting responsible, cost effective, efficient and timely lending decisions. Innovative lending solutions supported by screen scraping bring competition and choice to the market. Screen scraping also supports fraud prevention measures and compliance with the anti-money laundering and counter-terrorism financing legislation.

While the Consumer Data Right regime (**CDR**) offers an alternate mechanism for data sharing, non-bank lenders are not obligated to participate where their loan book remains below the de minimis threshold.<sup>2</sup> The de minimis threshold for mandatory CDR participation acknowledges the substantial

---

<sup>1</sup> Comparison based on the cost of borrowing \$1500 over 9 fortnights between the Wallet Wizard Smart Loan and small amount credit contract competitor. See comparison at <https://www.walletwizard.com.au/compare-us>

<sup>2</sup> Currently expected to be \$500M, as proposed.

compliance and cost imposts associated with CDR participation. Such imposts do not exist under a screen scraping model, which offers significantly lower entry costs.

Relevantly, the Treasury's non-bank lending sectoral assessment<sup>3</sup> recognised that the application of regulatory obligations at a time when smaller providers could not absorb the costs would stifle their potential to grow their business and bring competition.<sup>4</sup>

We consider that prohibiting screen scraping will increase costs for non-bank lenders and create barriers to entry. This will stifle innovation, reduce competition from emerging lenders, increase the cost of credit for consumers, and, contrary to the aims of CDR, reduce consumer choice.

A screen scraping ban will reinforce the existing information asymmetry between ADIs and non-bank lenders that CDR was designed to address, whereby ADI lenders will be in a competitively advantageous position as they already have access to the customer's data, without requiring permission.

We understand that data security is the most significant countervailing benefit in support of a ban. However, screen scraping has been conducted safely by financial service providers in every jurisdiction around the world for over a decade with no reported data security breaches globally.

The concerns relating to lenders holding internet banking login credentials of their customers is, at least in the most part, misconceived. Login credentials are not typically visible to, and are not typically collected by, lenders. Instead, these credentials are provided directly to the data processor through a plugin on the lender's website, without being captured by the lender.

Data processors engaged in providing screen scraping services are predominantly large and reputable data analytics companies, employing sophisticated information security protocols similar to those of banking institutions. Both lenders and entities conducting screen scraping have existing obligations to protect personal information under the privacy laws.

Prohibiting screen scraping is likely to lead to lenders, eager to maintain their competitiveness by avoiding the cost imposts and data disadvantages associated with the CDR regime, adopting manual or in-house developed workarounds to access and manipulate information necessary to assess loans. These workarounds are likely to heighten, rather than reduce, the risk of data breach.

Moreover there is a risk that certain lenders might seek login credentials directly from applicants, rather than through the existing secure plugins from reputable screen scraping providers. Such a practice would expose consumers to heightened risk, which will disproportionality affect the most vulnerable lower income consumers who have limited borrowing alternatives.

In the circumstances, there is no compelling argument favouring a ban.

As outlined in Treasury's final report into open banking, screen scraping should not be prohibited. Rather, the goal of opening banking should be to make the practice redundant by facilitating a more efficient data transfer mechanism over time.<sup>5</sup>

---

<sup>3</sup> Australian Government - Treasury, *Consumer data right: Non-bank lending sectoral assessment – Final Report*, August 2022, at 5.5 <https://treasury.gov.au/publication/p2022-300402>

<sup>4</sup> Australian Government - Treasury, *Consumer data right: Non-bank lending sectoral assessment – Final Report*, August 2022, at 5.5 <https://treasury.gov.au/publication/p2022-300402>

<sup>5</sup> Australian Government – Treasury, *Review into Open Banking: giving customers choice, convenience and confidence – Final Report*; December 2017 <https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-For-web-1.pdf>

## Responses to the Consultation Questions

We have included a response to some of the questions set out in the discussion paper below.

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

Credit Corp, through a third party data provider, is engaged in screen scraping of bank account data to support its obligations under the responsible lending laws. The availability of such services supports responsible, cost effective, efficient and timely lending decisions.

In addition, Credit Corp uses screen scraping to support our fraud prevention measures and our obligations under the anti-money laundering and counter-terrorism financing legislation. While CDR will provide access to transaction data, other relevant account information available through the screen scraping process allows us to validate applicant details to help us prevent application fraud.

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?*

Credit Corp currently employs screen scraping solely in relation to banking data.

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?*

Applicants provide internet login credentials via a plugin to our website application. Prior to providing information, consumers are made aware that their information will be collected, and are required to acknowledge and agree to a privacy disclosure and consent. In addition, any consumer who has elected to enable two-factor authentication with their financial institution will be prompted to approve access via the relevant secondary authorisation mechanism.

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

Credit Corp uses screen scraping solely for the purpose of data collection to assist with assessing credit applications to meet its responsible lending obligations and determine credit risk, mitigate fraud and comply with the AML/CTF legislation. Actions are not taken on behalf of customers.

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

Risk is mitigated where lenders do not collect or store internet banking login credentials and where they are instead provided directly to the data processor through a plugin on the lender's website, without being captured by the lender.

Data processors engaged in providing screen scraping services are typically large and reputable data analytics companies, employing sophisticated information security protocols equivalent to those of banking institutions including security certifications, such as, ISO27001 and SOC2, which involve independent verification of the systems and controls of the certified party.

The ACCC has acknowledged that while existing industry information security certifications may not demonstrate compliance with *all* of the controls required under the CDR regime, it is the ACCC's intention is to allow existing security certifications to be leveraged,<sup>6</sup> demonstrating their accepted value in data security.

---

<sup>6</sup> Australian Competition & Consumer Commission, *Consumer Data Right – Rules Outline*, December 2018, Table 1: Accreditation criteria (and continuing obligations on accredited data recipients) <https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf>

In addition, we understand that the key screen scraping service providers are also governed by the Privacy Act, the obligations of which are largely reflected in the Privacy Safeguards set out in the CDR Rules.

There are considerable controls in place which support the safety of screen scraping. Conversely, in the context of lending, a premature prohibition of screen scraping may force many smaller providers and market entrants to withdraw products from the market, or revert to more manual processes, for example, by relying on 'paper' based financial information in support of credit applications. We consider that such 'paper' based information is significantly more prone to the risk of fraud and financial abuse than screen scraping. It may also expose consumers to the risk of erroneous application outcomes owing to errors in manual review and categorisation of banking transaction data.

Moreover there is a risk that certain lenders might seek login credentials directly from applicants, rather than through the existing secure plugins from reputable screen scraping providers. Such a practice would expose consumers to heightened risk, which will disproportionately affect the most vulnerable lower income consumers who have limited borrowing alternatives.

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

None that we are aware of.

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

Screen scraping is available in all jurisdictions in which we operate, including Australia, New Zealand and the United States of America. We are unaware of any plans in those jurisdictions to ban such processes.

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

CDR aims to provide consumers with efficient access and use of their information. By doing so, we understand that CDR aims to enable consumers to maximise the value of their data and increase competition.<sup>7</sup>

However, CDR imposes significant costs and compliance burdens on lenders, which will disproportionately impact small and emerging lenders. Screen scraping has significantly lower entry costs.

Screen scraping offers the finance industry accessible point in time data. Such accessibility supports financial service providers in providing efficient and competitive consumer outcomes.

In Report 718,<sup>8</sup> ASIC correctly recognised the “*appropriate balance, allowing the use of potentially beneficial services to continue while industry gradually transitions to the CDR framework and as the regulatory and operational aspects of this framework gradually evolve*”.<sup>9</sup>

Any phasing out of screen scraping should be a natural consequence of open banking making the practice redundant by facilitating a more efficient data transfer mechanism. With CDR still in its infancy, this will occur only after full participation, development and enhancement of CDR has been achieved.

---

<sup>7</sup> *Treasury Laws Amendment (Consumer Data Right) Bill 2019 - Explanatory Memorandum*, see 1.3.

<sup>8</sup> Australian Securities & Investments Commission, *Report 718: Response to submissions on CP 341 Review of the ePayments Code: Further consultation (Report 718)*, March 2022 - <https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-718-response-to-submissions-on-cp-341-review-of-the-epayments-code-further-consultation/>

<sup>9</sup> Report 718, page 38.

Retaining screen scraping will allow the finance industry the continued opportunity to pursue business growth and innovation, promoting competition in the market. The alternative is likely to lead to increased costs to smaller and emerging credit providers, which will either be passed on to consumers in higher rates or fees, or otherwise reduce the competitiveness of these providers.

A ban on screen scraping may also cause lenders to rely on manual processes and/or seek login credentials directly from applicants (a data security risk) as an alternate to incurring the expenses associated with CDR. Applying more manual processes is likely to lead to errors in transaction classification, and may limit credit to consumers for whom the loan would have been suitable, or conversely result in the provision of unsuitable loans, in each case causing consumer detriment.

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?*

Screen scraping continues to provide an effective and broadly safe alternative, whilst CDR within Australia remains in its very early stages. We understand that only approximately 80 ADIs contribute to the CDR regime in its current format. Screen scraping facilitates access to a substantially greater number of providers.

While CDR provides access to transaction data of CDR participants which is likely to support a responsible lending assessment, we understand that balance data is not always available and that eStatements, which can be obtained through screen scraping, are not available under CDR.

We are uncertain whether all data currently relied on to mitigate fraud risk will be available under the CDR regime.

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 consider that Government should consider whether CDR is a viable alternative via an assessment of the relative full costs involved with implementing and managing CDR, together with the completeness of banking data relative to screen scraping.

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

There are compelling arguments not to ban screen scraping. Any phasing out of screen scraping should be a natural consequence of open banking making the practice redundant by facilitating a more efficient data transfer mechanism.

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

We do not support a ban on screen scraping within any timeframe, due to the cost and compliance imposts associated with CDR. As outlined above, any phasing out of screen scraping should be a natural consequence of open banking making the practice redundant by facilitating a more efficient data transfer mechanism

With CDR still in its infancy, this will occur only after full participation, development and enhancement of CDR has been achieved. We consider this will take many years to achieve.

## Conclusion

For the reasons set out above, Credit Corp considers that screen scraping continues to provide an effective and broadly safe alternative, whilst CDR within Australia remains in its very early stages.

It supports competition in the finance market with its accessibility to non-ADIs and to smaller and emerging providers, providing a lower cost alternative to CDR participation. Screen scraping also plays an important part in reducing fraud and supporting compliance with laws relating to responsible lending and anti-money laundering and counter terrorism financing.

Therefore, we consider that there are compelling reasons that screen scraping should remain available and that any phasing out of screen scraping should be a natural consequence of open banking making the practice redundant by facilitating a more efficient data transfer mechanism

Yours faithfully

A handwritten signature in black ink, appearing to read 'M. Angell', written over a thin horizontal line.

Matt Angell  
Chief Operating Officer  
Credit Corp Group