shift

24 October 2023

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

Screen Scraping Discussion Paper – policy and regulatory implications

Shift Financial Pty Ltd (**Shift**) appreciates the opportunity to provide feedback and comments on the Screen Scraping Discussion Paper dated August 2023.

This submission provides both general comments and feedback on screen scraping (**Section 1**) and responses to the specific questions in the Discussion Paper (**Section 2**).

About Shift

Shift offers a range of credit, payments and data solutions to business customers and their partners. Since its inception in 2014, Shift has provided over $2.5b to Australian businesses who are typically underserved given the complexity of small to medium enterprise (SME) lending – a large amount of which has been underwritten using transaction data provided digitally. Shift is headquartered in Sydney and has over 250 employees.

Executive Summary

Shift considers the ability for financial services customers (both individuals and businesses) to share their financial data with financial services providers both easily and safely is vital to supporting product innovation and competition dynamics in the market.

Shift also fully endorses the Government's desire to extend Consumer Data Right (CDR) to the non-bank lending sector with the goal of increasing the availability of data and encouraging innovation in financial technology.

However, given the current limitations of the CDR regime for data sharing in relation to business accounts and the significant compliance costs for participants, Shift contends:

- screen scraping must be retained as an option for customers to share data with financial services providers until such time as the CDR regime provides a sufficiently useful and cost-effective alternative for customers and financial services providers to share financial information; and

- the focus of any further legislative changes should be on addressing the limitations and usability of CDR data in the banking sector following continued consultation with industry.

Shift considers that this hybrid technology approach (with both screen scraping and CDR running in parallel during an appropriate transition period) best supports the provision of financial services to customers and competition dynamics in the market. In addition, it provides more time for government and industry to ensure open banking meets the intended policy objectives and the data needs of customers and CDR participants.

Section 1 – General comments and feedback

Currently, the use of screen scraping is prevalent in financial services as an easy and relatively safe option for customers to share their information with providers. Shift's business model is enabled by, and relies on, the supply of transaction data to support lending activities to Australian small businesses.

Shift's customer value proposition is centred on convenience and control with the goal of providing SMEs finance on demand. To undertake fast and accurate credit decisioning, Shift utilises banking data provided via screen scraping. The use of this technology has many benefits to our customers including:

- a uniform consent/authorisation experience;
- high connection reliability with low error rates;
- ability to accurately assess credit risk via real-time visibility of business accounts;
- fast decisioning; and
- a completely digital experience.

Without the availability of this transaction data via screen scraping, Shift would not have been able to, and would not be able to continue to, provide credit products to many small businesses which are typically underserved by the banks.

CDR data limitations

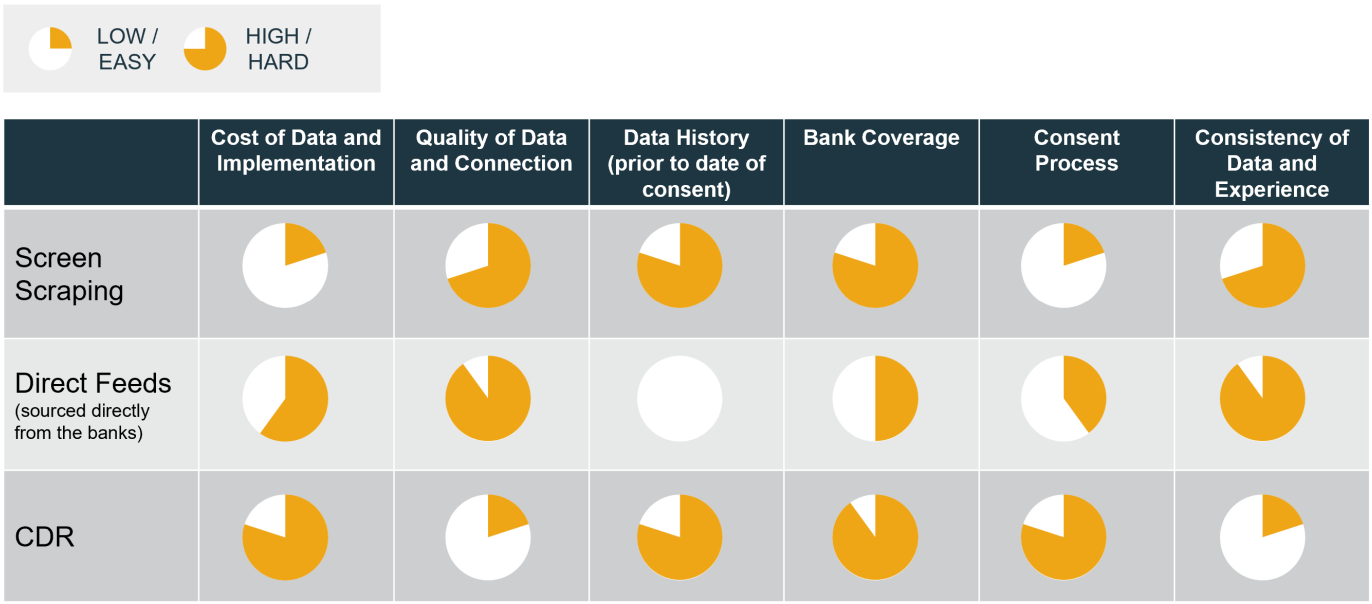
Shift has undertaken user testing of the CDR data provided by many data holders and has identified numerous issues with the quality and accuracy of the data provided via open banking and the consent and authorisation process. These issues are particularly problematic for data related to business accounts.

These include:

Data quality	Inconsistent and unreliable transaction data quality, particularly for business related accounts. For example, user testing showed that CDR account coverage often excludes accounts without reason (e.g. a transaction account will appear as ineligible and a business account may not appear at all).
Consent	Consent errors without explanation. For example, user testing showed an error page on two "Big 4" bank's website during the consent flow after entering the one-time password. In addition, data consent is not enduring. Therefore, it is unclear what the process is for consent extension where ongoing data is required.
Authorisation	Manual, non-digital customer authorisation/consent.

	For example, at least two of the “Big 4” banks require customers to download a customer consent form, complete the form manually and then return it to the bank.

Following detailed user testing, Shift undertook a comparison of the transaction data available via current technology options in market and this can be summarised in the diagram below:



In summary, the comparison demonstrates that screen scraping is a relatively cost-effective, reliable and accurate source of data that supports the provision of fast, digital financial services to SME customers. Shift is happy to provide further information on the results of its user testing on request.

In light of the information above, Shift believes that screen scraping must be retained as an option for customers to share data with financial services providers in parallel until such time as the CDR regime provides a sufficiently useful alternative for SME customers and financial services providers to share financial information with the accuracy, reliability and speed of screen scraping. Until the accuracy, reliability and speed of sharing CDR data is improved, screen scraping remains a critical mechanism to empower SME customers, support product innovation and facilitate competition in a cost-effective way.

Shift contends that Treasury should not consider banning screen scraping until the current issues with the CDR regime are addressed. Shift believes that banning screen scraping before these limitations are addressed will unnecessarily and significantly impede competition and innovation in the business lending segment, and ultimately negatively impact SMEs that are already underserved.

Based on the user testing conducted, Shift believes that if screen scraping is banned prior to these data limitations being resolved, it would be unable to provide digital lending to the majority of SMEs and would be forced to revert to paper based, manual credit assessments. This would result in significantly slower credit approvals and would severely undermine the ability of SMEs to access finance as needed.

CDR data items to be addressed

Shift believes the following items needs to be adequately addressed by the CDR regime prior to the banning of screen scraping:

1. market coverage of real time, fully digital, access to SME business accounts;

2. the current CDR exemptions for missing accounts should be removed;

3. a consistent authorisation and consent process must be adopted across the industry;

4. there must be mandatory SLAs in relation to the availability of data once customer consent has been provided (e.g. <5 minutes);

5. there must be user testing in the production environment which demonstrates enterprise level error rates (<0.001%) with a focus on missing accounts and consent errors; and

6. there must be enduring consent allowing data to be shared for the life of a product.

In addition, Shift contends that screen scraping provides an important benchmark to assess the performance of Open Banking. To this extent, the adequacy of CDR should be measured against the success metrics set out in **Annexure A** with appropriate benchmarks in each of the categories to ensure parity with the cost, accuracy, utility, reliability and performance of screen scraping.

Will the banning of screen scraping accelerate the utility of CDR?

The mandatory transition of non-bank lenders to the CDR regime and the banning of screen scraping will not address the current limitations in the CDR regime and will therefore negatively impact SME customers who may no longer be provided financial services by non-banks given the lack of reliable, real-time digital data.

Whilst some comparison has been made within the industry to the mandatory participation of banks into comprehensive credit reporting, Shift contends that it is not a reasonable comparison. Comprehensive credit reporting legislation required the mandatory participation of banks to contribute additional data elements (e.g. repayment history information) which facilitated better access to data for all consumer credit lenders. The change only related to the enhancement of available data. It did not in involve the banning of an existing service which provides reliable and accurate data and with which the industry is heavily reliant on.

Focus of further regulatory changes

Given the data quality and consent/authorisation issues with Open Banking, Shift believes that the focus of any further legislative changes should be on addressing the usability of CDR banking data (particularly for business accounts) as set out above following continued consultation with industry.There are potentially several ways to do this, including by establishing an industry body that is tasked with monitoring of compliance with open banking standards that have more prescriptive requirements and timeframes in relation to the consent process and the sharing of data from relevant accounts.

Security

The Discussion Paper has raised security of information as a key risk associated screen scraping. Shift agrees that security of customer information is of vital importance and ultimately, the goal should be sharing data easily and safely via the CDR regime. However, until such time that the CDR regime can adequately replace screen scraping, Shift contends that security of screen scraping should not be a driver to prematurely ban it given the lack of evidence in Australia that supports the contention that screen scraping

is unsafe for customers. To the best of our knowledge, no customer credentials have been compromised in Australia since the current screen scraping technology commenced over 10 years ago.

Section 2 – Specific Questions in Discussion Paper

Question 1	Response
What screen scraping practices are you aware of or involved in?	Shift uses screen scraping technology to provide customer's a fast, digital onboarding experience. Specifically, Shift accesses transaction data to assess a business's credit worthiness for a credit application both on an upfront and ongoing basis. It is also used for validating bank credentials for payments and to help reduce fraud on automated decisions. Shift is not aware of any screen scraping practices beyond what is set out in the Consultation Paper.
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?	Shift currently only uses bank transaction data (both individual and business). The scope and purpose of Shift's use of screen scraping includes: • underwriting including determining credit limits; and • determining payment details and account information.
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?	Prior to customers providing their bank details to Shift, customers provide express consent to Shift using a secure token from Illion to save and refresh bank statements reports and obtain account transaction details to assess and monitor loans. Customers also acknowledge that they understand that the account transaction details include any transactional data from any accounts linked to the login credentials which are provided to Illion. In addition, customers agree to end user terms and conditions provided by Illion (https://www.bankstatements.com.au/about/terms).
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? ?	Given Shift may offer businesses revolving credit lines, the customer agrees to an ongoing connection to the transaction data for some products. The connection is terminated when the credit product is closed. This is disclosed to the customer and the connection status is available to the customer.
Do you use screen scraping for purposes other than data collection?	No – only data collection for the purposes set out above.
Question 2	
Are there any other risks to consumers from sharing their login details through screen scraping?	Shift acknowledges the security concerns set out in the Consultation Paper. However, as noted above, Shift contends that security of screen scraping should not be a driver to prematurely ban it given its utility for customers and the lack of evidence in Australia that supports the contention that screen scraping is unsafe

	for customers. To the best of our knowledge, no customer credentials have been compromised in Australia since the current screen scraping technology commenced over 10 years ago. Shift clearly discloses the use of screen scraping to its business customers and maintains robust security controls in to ensure there is no use or disclosure of transaction data for any other purpose.
Question 3	
Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?	No – Shift has not had any breaches involving screen scraping and has no further information to provide on this issue.
Question 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?	Currently business banks (NAB Connect, ANZ Transact and Combiz) cannot be accessed via screen scraping.
Question 5	
Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping? (take actions on behalf of a customer)?	Shift partners with Illion to access transaction data. Illion ensures online banking credentials are encrypted. Data is encrypted with bank level 256-bit encryption secured by 2048-bit keys. Its services are independently tested and audited by external security experts.
Question 6	
Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?	Shift is not aware of any other regulatory reforms that impact screen scraping, beyond what is identified in the Discussion Paper.
Question 7	
Are there any other international developments that should be considered?	Shift is not aware of any other international developments that should be considered, beyond what is identified in the Discussion Paper.
Question 8	
What are your views on the comparability of screen scraping and the CDR?	Please see Shift's submission in Section 1.
Can you provide examples of data that is being accessed through screen scraping that cannot currently be accessed using the CDR or vice versa?	As noted in Section 1, user testing has identified that CDR account coverage often excludes accounts without reason (e.g. a transaction account will appear as ineligible and a business account may not appear at all).
Are there particular restrictions related to data use and disclosure under the CDR that influence choices to continue using screen scraping, or vice versa?	The lack of clarity around enduring consent to access CDR data. Shift's business model is enabled by, and relies on, the regular supply of transaction data to support lending activities to Australian small businesses for some revolving credit products.
Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?	The UK approach to Open Banking has been effective in ensuring consistency and utility of data via the monitoring of compliance with open banking standards by the Open Banking Implementation Entity (OBIE) and by ensuring the focus of data sharing is highly effective in payments and banking data before roll-out to other sectors.

	Shift considers that the legislative focus should be on taking steps to improve the current utility of CDR in banking prior to either rolling it out to other sectors or banning screen scraping.
Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?	Please see Shift's submission in Section 1.
Question 9	
The Statutory Review recommended that screen scraping should be banned in the near future in sectors where the CDR is a viable alternative. How should the Government determine if the CDR is a viable alternative?	Please see Shift's submission in Section 1 and the recommended performance metrics set out in Annexure A.
What are your views on a ban on screen scraping where the CDR is a viable alternative?	Shift opposes the banning of screen scraping until the current issues with the CDR regime are addressed. Shift believes that banning screen scraping before these limitations are addressed will unnecessarily and significantly impede competition and innovation in the business lending segment, and ultimately negatively impact SMEs that are already underserved. See Shift's submission in Section 1 for further information.
What timeframe would be required for an industry transition away from screen scraping and why?	Given the significant costs and burden of implementing Open Finance as both a data holder and data recipient, Shift believes that organisations should be provided at least 12-24 months to transition away from screen scraping (and only once industry participants are satisfied that CDR is a viable alternative). The banning of screen scraping and a forced transition to Open Finance will have significant impacts on non-bank lenders and fintechs. There are both significant costs and complexity to do this. Some of the work will include: • retraining credit assessment models; • new staff/teams for Open Finance transition; • appointment of new supplier/s to support Open Finance; • changes to customer onboarding experience, customer contracts, consents, disclosures and privacy policies; and • changes to the customer portal. A project of this size will likely negatively impact other product development, investment into non-bank lenders/fintechs in a challenging macro-economic environment and ultimately, the ability of non-bank lenders/fintechs to meet customer's needs. Whilst Shift intends to integrate CDR data into its current product construct to replace screen scraping where appropriate, attempting to concurrently integrate data from the framework and share information back to other recipients will limit the ability to fully utilise CDR

	information to support customers. Shift's view is that screen scraping should not be banned until such time that CDR provides a via alternative from both a data utility and cost perspective.

Shift thanks Treasury for the opportunity to consult on the Discussion Paper.

Yours sincerely

Jamie Osborn CEO, Shift
Jamie.Osborn@shift.com.au

Annexure A – Recommended success metrics to be developed for CDR data prior to the banning of screen scraping

Centralised Processes and Data Quality	• Standardised consent and authorisation across the banks, account types, and authorising parties. • Creation of an industry body that monitors data quality and oversees self-regulation.
Technology	• Fully digital technology solution to support digital operating models. • A clearer view for the data recipient of what data is not being shared by data holders.
Consistent	• Consistent use of the payload by bank. • Consistent accreditation process.
Multi-Party Sharing	• Clarify the delineation between personal and business (while understanding SMEs will often not have a clear delineation between personal and business). • Create certainty around sharing "obligations" with third parties e.g., brokers and accountants.