Screen scraping – policy and regulatory implications

Cash Converters discussion paper response

August 2023

Executive Summary

In response to the Australian Treasury's August 2023 discussion paper on the regulation of screen scraping (The Australian Government, Screen scraping – policy and regulatory implications, 2023), Cash Converters is keen to submit its observations and responses. Our business heavily relies on screen scraping technology to efficiently identify and assess customers during loan application processes. This technology is not only critical in streamlining our operations but also plays a vital role in ensuring a satisfactory customer experience and avoiding financial exclusion which could occur with abrupt transitions to new technologies.

Cash Converters acknowledges that the shift from screen scraping to open banking is inevitable. We support this transition but emphasise the necessity to maintain a balance that ensures good customer experience and accessibility to credit products are not compromised. It is essential to approach this transition with a strategy that accommodates both the current functionalities provided by screen scraping and the potential benefits of the Consumer Data Right (CDR), thus fostering a seamless progression towards a more secure and efficient financial service landscape.

The following document contains Cash Converters responses, to the questions posed in The Treasury's discussion paper.

This includes recommendations to improve CDR data quality and processes, introduce governmental monitoring, incorporate critical institutions like MyGov, and streamline access for advisors and franchisees to enhance compliance and user experience.

Contents

Discussion Paper Questions & Response

Question 1 - How is screen scraping currently used?

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

Cash Converters, its subsidiaries and franchise network (collectively, "The Group") use screen scraping technology to collect information from applicants of consumer credit products (e.g., personal loans, car loans).

1a) Scope

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 data collected by screen scraping is used for two key purposes:

1. Know your customer (KYC) verification, an obligation under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF)
2. Affordability & unsuitability assessment, an obligation under the *National Consumer Credit Protection Act 2009* (NCCP).

Screen scraping is used to collect information from Australian Deposit-taking Institutes (ADIs) (e.g., banks and credit unions), as well as from MyGov (e.g., Centrelink).

The scope of the data collection is detailed in the following table:

Data Scope	Type	Source	Purpose
Bank transactions (90 days)	Structure data	ADI	Affordability assessment & assessment of unsuitability
Bank account holder name & address	Structure data	ADI	KYC verification
Centrelink income statement	PDF	MyGov	Affordability assessment & assessment of unsuitability
Centrelink income, deductions & emergency payments	Structure data	MyGov	Affordability assessment & assessment of unsuitability
Centrelink account holder name & address	Structure data	MyGov	KYC Verification

1b) Process

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?

The process is initiated by consumers through either a business-to-customer channel (B2C) or a business-to-business channel (B2B). When transacting on a B2C basis, the organisation provides information to consumers regarding screen scraping, its purpose, the terms and conditions and our privacy policy. When transacting on a B2B basis, the broker or dealer organisation has its own processes for communicating with consumers and privacy policies. A high-level overview of each process is included below.

Business to Customer Process

Consent
- Consumer is provided critical information (e.g. purpose of data collection, T&Cs, privacy policy)

ADI
- Consumer selects ADI from a searchable list of banks and credit unions
- Consumer provides necessary credentials (e.g. username, password, pin)

Screen scraping
- Credentials are transmitted to 3rd party intermediary, who "screen scrapes" information from the ADI customer portal

MyGov
- Consumer is asked if they are a recipient of Centrelink benefits
- If yes, consumer provides MyGov credentials

Screen Scraping
- Credentials are transmitted to 3rd party intermediary, who "screen scrapes" information from the MyGov portal

Data Collection
- The ADI customer data, and MyGov data (if relevant), is then collected by Cash Converters from the 3rd party intermediary
- The data is utilised to verify the consumers identity and assess their credit application

Business to Business Process

3rd party process
- Consumer engages a Broker or Dealer seeking a credit product
- Broker or Dealer direct consumer to use 3rd party intermediary to provide bank statements

Screen scraping
- Consumer provides necessary ADI credentials (e.g. username, password, pin)
- 3rd party intermediary "screen scrapes" information from the ADI customer portal

3rd party collection
- The ADI customer data is then collected by the Broker or Dealer from the 3rd party intermediary
- This includes a consumer "document ID", which can be passed to credit providers

Credit enquiry
- Broker or Dealer submits credit enquiry to lender, including the consumer "document ID"

Data Collection
- Credit provider (e.g. Cash Converters) downloads consumer bank statements from third party intermediary using the supplied consumer "document ID"
- The data is used to verify the consumers identity and assess their credit application

1c) Ongoing access

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?

Consumer data is accessed as a one-off at the time of assessing a loan application to review point-in-time transaction data as well as completing KYC verification. The Group do not access consumer data on a longer-term or ongoing basis.

1d) Actions on behalf of a consumer

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

The Group requires read only access., it does not use screen scraping to take actions on behalf of consumers.

Question 2 – Screen scraping risks

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

The Group has not independently identified risks beyond those already covered in the discussion paper.

Question 3 – Case studies

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

None identified.

Question 4 – Blocking

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?

There are two notable examples where consumers are blocked from using screen scraping: Bank of New Zealand (BNZ) and Up Bank. Consequently, these consumers are unable to apply for credit products with The Group.

Question 5 – Risk management

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

The Group has adopted the Office of the Australian Information Commissioner (OAIC) Privacy Management Framework and the NIST Cyber Security Framework (NIST CSF). Several risk mitigations have been implemented to reduce consumer risk:

- The Group does not store consumer credentials.
- Applicable partners have independently verified cyber security certifications (e.g. SOC2 & ISO27001).
- The network communications between consumers and partners are appropriately encrypted.
- The relevant systems are subject to annual independent security penetration testing.
- The relevant systems are subject to daily vulnerability scanning.

- Security patches/updates are regularly applied to both operating systems and applications. Critical priority security patches/updates are applied within 48 hours to both operating systems and applications. A device management platform is used to centrally orchestrate the application of security patches.
- Obsolete components that are no longer supported by a vendor/supplier are not used within the IT environment.
- Standard security configuration specifications are maintained and applied to servers, workstations, laptops and mobile devices. The granularity of these specifications is aligned with the device and user roles that are present in the organisation, for example a configuration for employees of HR are different for the employees of IT. The secure configuration follows a least-privilege model where services/features that aren't necessary for the role are disabled/blocked.
- Monitoring is configured and maintained to notify security incident responders of suspicious activity.
- The Group does not disclose collected information to other parties, except where lawfully required (e.g. AUSTRAC suspicious matter reporting).
- The Group does not use the collected data for purposes other than that for which it was collected (e.g. identifying consumers & assessing loan applications)
- In a B2B context, lenders can only access documents if they are appropriately "whitelisted" by the brokers/dealer.

Question 6 – Other Reforms or Legal Frameworks

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

The Group is aware that on February 16, 2023, the Attorney-General publicly released the Privacy Act Review Report, which includes 116 recommendations based on 30 "key themes and proposals" from stakeholders during the last two years. The report has put forward 116 proposals that, if implemented, will be the most dramatic change to the Australian privacy and data protection landscape since the introduction of the Australian Privacy Principles (APPs).

One of the key themes of the report is consent. The report recommends that consent must be informed, voluntary, current, specific, and unambiguous. The report also recommends that the OAIC develops guidance for online services in developing consent requests.

As highlighted in Question 1, the use of screen scraping within The Group, has arisen through, and been driven by, a need to meet obligations under the AML/CTF and NCCP Acts.

- Under the AML/CTF Act, providers of designated services are required to verify the identity of consumers, and the authenticity of information provided.
- Under the NCCP Act, credit providers are required, for certain product classes, to collect ADI transaction records (e.g. 90 days of bank statements).
- Under the NCCP Act, credit providers are required, for certain product classes, to collect Centrelink Income Statements.

Question 7 – International Developments

Are there any other international developments that should be considered?

The United Kingdom which pioneered the adoption of Open Banking globally (Competition and Markets Authority, 2021) has over 5 million active open banking users or approximately 10.6% of the

country's banked population (Sifted, 2022). The Group understands that under this relatively mature Open Banking regime, screen scraping technology is not yet prohibited by law (Liu, 2021).

Banning screen scraping prior to CDR technology reaching a suitable maturity level, reliability and adoption rate, risks unintended consequences (e.g. the financial exclusion of consumers), which would seem counterproductive to Open Banking's stated benefits (e.g. enhancing competition, innovation and consumer choice) (The Australian Government, Review into Open Banking in Australia - Final Report, 2017).

Question 8 – Screen Scraping & CDR Comparability

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

The Group considers that over time, the CDR will be compatible with screen scraping. However, it is currently plagued by a lack of quality assurance, which affects the availability and quality of data. While some of these issues may seem trivial, The Group has evidence demonstrating that it takes a long time for these issues to be addressed. The following table contains a list of illustrative examples.

CDR Issue	**Impact**
Bankwest, unit number omitted from account holder address information – reported on the 16/03/2023, fixed on 02/08/2023 **(139 days to resolve).**	The impact of this issue is that CDR could not be used to meet AML/CTF obligations (KYC) for affected consumers. During testing, the full address information for Bankwest customers was available through screen scraping solution providers.
Commonwealth Bank, user testing indicated that authentication and authorisation of CDR requests was inconsistent/unreliable, with some consumers not receiving the relevant authentication notification in the Netbank mobile app. **(retested 29/09, resolved)**	CDR could not be accessed to meet AML/CTF or NCCP obligations for affected consumers. During testing, Commonwealth Bank information could be provided by screen scraping technology providers.
Bendigo Bank, user testing indicates that account information is unavailable, this is an on-going issue. **(unresolved)** User message: "You don't have any eligible accounts to share data with Cash Converters Personal Finance Pty Ltd". Error message: *"We're sorry, something went wrong. We're working to fix the problem. Please try again later, or contact [XXXX] for urgent assistance."*	CDR could not be accessed to meet AML/CTF or NCCP obligations for affected consumers. During testing, Bendigo Bank information could be provided by screen scraping technology providers.
Westpac, routing number and account number has been conflated into a single field. **(unresolved)**	The Group is unable to adequately verify banking information for the affected consumers. The BSB and account number is provided separately by screen scraping technology providers.

8a) Data access

Can you provide examples of data that is being accessed through screen scraping that cannot currently be accessed using the CDR or vice versa?

Yes, there are several examples:

- There are critical institutions (e.g. Department of Human Services (DHS) / MyGov) that do not participate in the CDR regime.
- Our testing has identified that critical information, such as account holder name and account holder address, is not consistently provided by some institutions under CDR regime.
- There are several institutions (BNZ and Up Bank) understood to block screen scraping.

8b) CDR restrictions

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 Group is currently aware of two possible restrictions under the CDR.

Sharing data with franchisees.

The Group includes a network of franchisees that provide consumer credit under the NCCP and thus each independently hold an Australian Credit License (ACL). There are three CDR access models most relevant to providing credit under an ACL.

Access Model	Data Sharing	Accreditation
Accredited Data Recipient (ADR)	Suitable for entities that need to share CDR data	Highest level of accreditation
Sponsored Affiliate	Not suitable for sharing CDR data	Accreditation with an ADR acting as a sponsor
Principal & Representative	Not suitable for sharing CDR data	No official accreditation required

The Group is engaging with its partners and the ACCC to determine the most suitable access model, however, our current understanding is that The Group will need to seek full accreditation (ADR) to facilitate the necessary sharing of information within its franchise network. There are several scenarios that exemplify why this is required.

- Franchisees use Cash Converters systems to provide credit assistance to consumers who visit their outlet seeking to apply for Cash Converters Personal Loans.
- Franchisees use Cash Converters systems to provide credit directly to consumers using under the Franchisee's ACL.

Brokers sharing data with credit providers.

The Group has a network of affiliates (e.g. finance brokers and car dealers) that provide consumers information and advice about financial products. Once a consumer decides to proceed with a loan application, with the advisor acting as a representative, screen scraping information (e.g. bank statements) is typically shared with the credit provider as part of that loan application. We understand that these affiliates are able to collect CDR data under the "Trusted Advisor" access model, however, it

is not clear whether these Trusted Advisors can in turn share the CDR data they collect with relevant credit providers on behalf of the consumer as part of a loan application.

8c) Other regulatory restrictions

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

There are two main regulations that affect the viability of CDR as an alternate to screen scraping.

1. AML/CTF – KYC information is not consistently and reliably provided by the CDR currently (e.g. account holder name and address)
2. NCCP – MyGov data is not currently included in the CDR (e.g. Centrelink Income Statements)

8d) Suggestions

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

We have several recommendations:

Recommendation	**Why**
The quality control of CDR data, specifically account holder details and information, must be improved.	Currently, CDR can't be relied upon to meet AML/CTF and NCCP obligations.
The CDR authentication, authorisation, and consent processes must be improved.	We've noted many inconsistencies and reliability issues in the way institutions treat consumer consent. For example, consumers facing onerous consent options, or mobile app authentication processes simply not working.
The Government should implement systematic monitoring of data quality and authentication success and consent rates.	If institutions authentication or consent rates are unexpectedly low, it is likely indicative of an underlying technology or user experience problem. Having this monitoring in place will allow access quality to be measured objectively. e.g. organisation A's consent rate is 50% vs organisation B's 90%; why?
The Government should consider the need for critical institutions (e.g. MyGov) to be included in the CDR.	The CDR can't be used currently to meet all NCCP obligations, such as collecting Centrelink Income Statements for the assessment of loan applications for certain financial products.
There should be further streamlining of trusted advisor access models, allowing the sharing of information with ACL holders (e.g. when applying for consumer credit).	Without this, consumers may face additional barriers when seeking credit solutions through brokers, potentially having to provide consent several times, for different entities, at different stages, throughout a loan application process.
There should be further streamlining of access models for franchisees, or extended timeframes for franchisee business models to adapt their business models to the current CDR access models.	Some existing business models may not be viable under the current CDR framework (e.g. franchisees accessing and sharing data with a franchisor).

Question 9 – Statutory Review

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

9a) Government determination

How should the Government determine if the CDR is a viable alternative?

More needs to be done to better guarantee data availability and data quality. This should include:

1. Systematic monitoring of authentication & authorisation success rates (e.g. if one institution authentication or authorisation rate is lower than others, it is likely indicative of an underlying technology problem).
2. Systematic monitoring of data quality (e.g. consistent availability of account holder information).

In addition, the Government should consider the role of Government data holders (e.g. DHS and MyGov) in the CDR regime.

9b) Is CDR a viable alternative?

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

The Group sees a transition to CDR as inevitable, however, believes that this will occur organically, as the CDR data quality and platform reliability improves. Screen scraping should only be banned once the CDR adoption rate reaches a critical mass.

9c) Transition timeframe

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

Forcing an industry transition prior to the CDR meeting relevant reliability and quality criteria would counter the stated benefits of Open Banking (The Australian Government, Review into Open Banking in Australia - Final Report, 2017) and risks the financial exclusion of impacted consumers and significant disruption to industry.

Considering the results of on-going testing, the observed rates of improvement and the highlighted complexity with CDR access (e.g. for Franchise, Broker & Dealer networks), The Group believes that a full transition for ADI (e.g. bank statements acquisition) is 24-36 months away. The Group's current internal objective is to transition 10% of ADI data acquisition to CDR by 30/06/2024.

References

Competition and Markets Authority. (2021, November 5). *Update on Open Banking*. Retrieved from GOV.UK: https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking

Liu, H.-W. (2021, April 23). *The Legality of Screen Scraping and Its Open Banking Moment*. Retrieved from Faculty of Law Blogs, University of Oxford: https://blogs.law.ox.ac.uk/business-law-blog/blog/2021/04/legality-screen-scraping-and-its-open-banking-moment

Sifted. (2022, April 5). *The state of open banking in Europe*. Retrieved from Sifted: https://sifted.eu/articles/state-europe-open-banking-uk-fintech

The Australian Government, T. (2017, December). *Review into Open Banking in Australia - Final Report*. Retrieved from The Treasury: https://treasury.gov.au/consultation/c2018-t247313

The Australian Government, T. (2023, August 30). *Screen scraping – policy and regulatory implications*. Retrieved from The Treasury: https://treasury.gov.au/consultation/c2023-436961