



25 October 2023

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

Classification: Public

Via email to: data@treasury.gov.au

Re: Cuscal response to Treasury’s consultation on Screen scraping – Policy and regulatory implications.

Cuscal Limited (Cuscal) welcomes the opportunity to provide feedback on the discussion paper on Screen scraping – policy and regulatory implications.

The data aggregators in Australia generally use screen scraping technology to collect information, in the absence of any direct feed arrangements with financial institutions. This practise has been in place since 2001 as noted in [ASIC’s Consultation paper](#). While this practise helped the financial sector in the early years, the introduction of Consumer Data right regime in 2019 followed by the implementation of Open Banking in 2020 has now made available a more robust, trusted mechanism for consumer data sharing. Cuscal maintains its position to support a ban on Screen scraping in the financial services sector where CDR is a more viable option for consumers.

Background to Cuscal

For over 50 years, Cuscal has leveraged our assets, licensing, and connectivity to provide intermediary and principal outsourcing activities on behalf of our clients. We are an end-to-end payments specialist that services more than 100 established ADI and challenger brand clients within Australia's financial system, including the majority of the mutual banking sector, and a growing number of FinTech and 'PayTech' enterprises. We enable their market connectivity so they may provide innovative products, business models, and drive improved customer outcomes.

We are an Authorised Deposit-taking Institution (ADI), the holder of an Australian Financial Services Licence, and an Australian Credit Licence for Securitisation purposes. Cuscal has Board representation with Australian Payments Plus, NPPA, BPAY, Eftpos, the Australian Payments Network and participates in numerous industry committees. We are also the founder of 86400 (rebranded to ubank, <https://www.ubank.com.au/>), a fully licenced mobile-led digitized bank, acquired by National Australia Bank.

The services that we provide to our client institutions include card scheme sponsorship for issuing and acquiring, payment card issuing, card production services, digital banking applications, access to domestic payment services using direct entry, BPAY, the New Payments Platform (NPP) and Open Banking platform services. We also act as settlement agent for many of our clients through our Exchange Settlement Account with the Reserve Bank of Australia (RBA).

As a fully PCI-DSS accredited ADI, Cuscal is uniquely placed to provide secure and robust capabilities that facilitate access to markets that would otherwise be beyond the reach of some organisations.





Cuscal's Role in Open Banking

Cuscal considers itself as a CDR Intermediary, helping entities to comply with the Consumer Data right regime and support their customers to obtain the most out of the data sharing regime.

Cuscal supports:

- ❑ Data Holders to manage compliance effectively.
- ❑ Consumers to share their banking data with best-practice simplicity, while remaining in control over the data they consent to share via their bank.
- ❑ Entities with technology services by minimising the time, cost, and risk of doing it themselves.

Cuscal has attained accreditation as a data recipient and successfully launched the myCDRdata service in July 2023. The myCDRdata service is an Industry-first tool that supports Data Holders with meeting their compliance obligations by providing functionality to test their CDR build in a production environment.

For further information on Cuscal and its services please refer to our website at www.cuscalpayments.com.au

Over the past two decades the Screen scraping practises used to extract content from third party websites have found countless applications. The data scraping technology existed and flourished due to the lack of an alternative for sharing data between banks and third-party entities. Today, the CDR is a more powerful mechanism for secure data sharing across various sectors and supports a number of consumer focussed use cases. More importantly, it has defined data ownership by the consumer and the right to access their own data.

The CDR should be preferred channel for data sharing practises given the robustness of the CDR legislation and accreditation processes. The ACCC, as the accreditation regulator, assesses the accreditation application and has historically declined certain applications due to lack of adequate security measures put in place by organisations. Screen scraping on the other hand is unregulated and requires the sharing of login details which, by nature, is not secure. Further cyber awareness programs and training warns consumers against sharing of their login details to safeguard themselves from scams and cybercrime. As such, it is evident that consumers would naturally be inclined towards safety and prefer to opt for channels that have consumer protections embedded. ASIC noted in its ePayments code review that consumers use screen scrapers at their own risk. Security is paramount with respect to sharing financial data across the economy.

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

Joint and complex accounts: The CDR regime balances the control each Joint account holder has over their accounts. This is managed through the Consumer dashboard, Disclosure Option management service (DOMS) and specific notification requirements on Data Holders. Such safety nets are non-existent in Screen scraping methods, leading to increased Privacy risk in Joint and complex account settings. The CDR regime has introduced robust data sharing practises such as explicit informed consent, consent management, Data minimisation, Data deletion, Consumer dashboard and Notifications for alerting data sharing activities. These measures are consistent across CDR participants and helps build standardisation in safe Data handling practises.





Privacy risk is a key concern associated with Screen scraping techniques. As the government looks to build and promote trust in the CDR ecosystem the risks associated with Screen scraping becomes more evident for consumers and the lack of consumer protections becomes a critical conversation. Screen scraping practises run counter to every piece of security advice provided by the government.

The **liability framework**, resulting from unauthorised access, is unclear in screen scraping services, exposing consumers to a high degree of uncertainty when seeking compensation options. There are additional concerns about cybersecurity, data breaches where login credentials are shared for scraping customer identifiable and financial data. The sharing of login credentials also provides write access to the accounts. The promise of Open Banking was to moderate such concerns and reduce the need for unofficial, unregulated standards such as screen scraping technology.

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

Use of Screen scraping could lead to a breach of contract terms under Australian laws for e.g.: violation of MyGov's terms of use. The digital Identity Bill is in proposal stage and is set to establish a nationally regulated system for access to both public and private sectors. Using screen scraping for sharing MyGov credentials could have widespread implications given the associated security risks involved. The screen scraping technology is considered as a cost-effective tool given its unregulated nature. However, a balance must be struck when managing Privacy and security of consumers.

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

The consultation paper highlighted the proposed reforms to responsible lending obligations. It should be noted that CDR is an economy wide reform, and the ecosystem is preparing itself to roll out in the non-bank lending sector along with the introduction of Buy Now Pay Later products as eligible product types. Given these imminent changes, it is arguable that CDR will be the safest route to data sharing for Consumers when compared to Screen scraping techniques, which existed when there were no other alternate channels for data sharing with third parties.

Last month Treasury released a consultation paper on Consent review and Operational enhancements in CDR. The discussion paper proposes the concept of bundled consent which pertains to combining CDR consents with non-CDR permissions. The non-CDR permissions can include practises such as screen scraping techniques. To maintain a high degree of security and safety in the data sharing economy it is important that unregulated non-standard practises like screen scraping is banned to provide more certainty to consumers.

Furthermore, as the CDR and Digital economy matures with the passage of Write access in CDR (action initiation) and the Digital Identity Bill, the stakes start to get higher. Practises such as screen scraping have no fixed standards i.e. each provider entity has its own approach and differing levels of security which is not regulated.

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

The approach taken by EU and UK with respect to banning screen scraping for Third party providers impersonating as customers via screen scraping is worth noting. On 19 October 2023 the Consumer Financial Protection Bureau (CFPB) proposed a rule that would accelerate a shift towards open banking in the United States. Open Banking is a mechanism to give consumers control over their data and gain new protections against companies misusing their data. Australia has a regulation-





based data sharing framework in the form of CDR regime which is a point of reference for other jurisdictions.

As open banking develops around the world, the practise of unregulated, unsecure data sharing will start to diminish, paving the way to increased consumer expectations around inherent data security in products and services.

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

□ **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?**

CDR provisions the sharing of key information related to a consumer including financial datasets in the Banking sector, except for Date of birth. In principle, datasets accessible through screen scraping should also be made available in CDR if deemed critical for providing the services. This will help bridge any gaps and support the viability of CDR above screen scraping techniques. What CDR prohibits is the sharing of sensitive login credentials and financial hardship data, which is required to protect consumers from risk of harm. However, we have not been made aware of any such examples that state specific datasets are missing in CDR. Largely, the perception of the industry has been the need to maintain high quality data shared through CDR. The work that ACCC is currently focussed on would help to make the necessary improvements in this area and bridge any gaps that exists in the quality of data shared in CDR.

□ **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?**


The key datasets required for providing a financial service have been accounted for in the CDR regime, except for Date of Birth. However, for a consumer to be eligible for Consumer data sharing in CDR they must be above the age of 18 years. There may be a need to identify the age of the consumer to ensure a financial product is designed for a specific age demographic under the target market determination requirements. As CDR expands in the Open Finance sector with Superannuation and Insurance sector assessments, the need for identifying a consumers age will become important for providing the required services.

There have been numerous articles previously with respect to missing datasets in CDR. It is important to understand the underlying issues as opposed to taking a generic view that CDR does not provide the level of detailed information as screen scraping technology. Primarily we believe this dialogue exists due to the data quality issues reported by CDR participants and ACCC is actively monitoring and prioritising this area as part of its compliance activities. The issues around screen scraping techniques are that it allows a third party to view a consumer's banking page, which is private to the consumer and has no reliance on the product or services consumed. This raises the privacy concerns which is of utmost importance when considering the type of data transmission.

However, we recognise that there are sectors that are yet to be assessed and designated, i.e. Superannuation, where screen scraping is prevalent. Until such time that these sectors transition to CDR regime, the only viable option is screen scraping in these sectors. However, when CDR is a viable option, it must be the compliant channel for all.

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





We are not aware of any current regulatory frameworks that affect the viability of CDR as an alternative to screen scraping. Our general view on this is CDR is the safest viable option for a data sharing economy as its regulated and secure. The entities handling the data are recognised within the regulation and must meet security standards, building the necessary trust within the ecosystem. The screen scraping technology cannot give the same degree of safety that exists under CDR, as entities relying on data scraping may not have the same levels of extensive systems and internal checks to ensure consumer credentials are safeguarded with utmost privacy.

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

The CDR framework is constantly going through reviews and improvements to make it the preferred choice for consumers to securely share data. A number of enhancements are in progress such as the CDR Consent review, Operational enhancements, authentication uplift, accessibility improvements to make the regime stronger. The ACCC is proactively looking at data quality within CDR as one of its key compliance measures to help with data consistency and help eliminate concerns raised by accredited data recipients. The representative arrangements, business consumer consents and outsourcing models in the CDR framework has been uplifted to allow for easier participation. We believe as the CDR ecosystem establishes across other sectors and participation increases, the framework will continue to evolve.

□ **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?**

The current process of engaging with the CDR ecosystem via Consultation process and engagement with impacted organisations will help support the transition process to CDR. Understanding what is the main deterrent to transitioning to CDR and how the government can help support ease these issues for service providers. A number of actions are being taken by Treasury, ACCC and OAIC in this direction and believe that engagement with the industry will help move towards the desired state where security is paramount in dealings with consumers financial data.

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

From a regulatory and policy perspective, Cuscal supports the view to ban screen scraping where CDR is a viable option. This is a no brainer given the current cyber threat environment and the security that CDR regime offers to consumers and businesses alike. A high-level comparison between these two data sharing options helps determine this position:

- The prevalence of screen scraping normalises the sharing of confidential consumer credentials to a third party. CDR regime does not engage in sharing of any sensitive login details with third parties, keeping the consumer interactions safe, always.
- The consent rules are embedded in the *Competition and Consumer (Consumer Data Right) Rules 2020* and drives the CDR regime. The same degree of control is not available under screen scraping methods and lacks consent management practises. The loss of control for a consumer is noticeable whereas CDR provides the consumers with absolute power to determine whom they share their data with, when they share and how long it is shared.
- Website terms and conditions may be breached by Consumers when sharing their login details with third party screen scrappers. For e.g.: Banks terms & conditions and Mygov terms of use.



- The standardisation of security and privacy requirements as part of the accreditation model sets a clear expectation on entities handling consumer data. Such streamlined regulations and requirements are missing in screen scraping technology and it is up to the organisation to have a high standard of risk management framework. The screen scraping practises gives unrestricted access and control to consumers financial accounts and associated data. It is noted that the small business exemption that currently exists in the Privacy Act 1988 is under review for removal and will help strengthen how Australian businesses protect consumer privacy.

However, Cuscal also recognises there are a number of organisations that function on the screen scraping technology and a ban might disrupt these businesses and their viability to function and support Australian economy. As such our recommendation is to give an appropriate timeframe for the small to medium businesses relying on screen scraping to transition to the CDR regime.

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

As the CDR regime expands into the Open Finance sector with non-bank lending data sharing soon to commence, it will help bridge the gap of consumers financial information available within the CDR ecosystem. With other sectors, Superannuation and Insurance to join CDR ecosystem in the future, it will overcome the barriers that screen scrapers have stated with respect to available financial data in CDR. We also recognise that data quality and responsiveness are some of the issues raised by FinTech's which are slowly but surely finding traction with the regulators to make CDR regime the preferred channel for data sharing prospects. It is important to note the longer screen scraping continues to exist, there will be inertia to take up CDR due to its regulatory nature and higher standards of security and privacy requirements on service providers. Cuscal is in agreement that removing high risk practises such as screen scraping from financial sector will help promote resiliency of our financial systems. We propose that Treasury looks at an adequate timeframe to help transition businesses that rely on data scraping technologies with a defined cut-off date.

In conclusion, Cuscal supports the discussion paper on screen scraping ban. A timeline for transition should be provided, however, it should be cognisant of the challenges faced by impacted organisations in the transition from one technology to another. Screen scraping technology existed due to the lack of a better alternative, however with a regulated data sharing regime in place this discussion paper is timely and important for advancing the CDR regime further. We look forward to discussing our submission with you should there be any further clarifications required.

If we can be of any further assistance in the interim, please feel free to contact me at kmckenna@cuscal.com.au or (02) 8299 9000.

Yours sincerely,

Kieran McKenna
Chief Risk Officer

