Australian Banking Association

Screen Scraping Consultation

Submission to Treasury

27 October 2023

Australian Banking Association

Table of Contents

Key Recommendations 2
ABA Submission on Screen Scraping 3
Viability: A comparable customer experience 3
Proposed Government retirement plan 4
Responses to Detailed Consultation Questions 5

Australian Banking Association

Key Recommendations

- Given the significant resource investment to establish the CDR by industry and government, this submission is made with the strong recommendation that Treasury prioritise their consideration of a cost-benefit analysis of not only new CDR initiatives (including improvements to the Standards), but the overall success of the CDR policy itself.

- The ABA broadly endorses the recommendation from the CDR Statutory Review that screen scraping be banned *where the CDR is a viable alternative*. To make the CDR a viable alternative, it needs to offer a comparable customer experience to screen scraping. To date, many of the previously implemented and currently proposed changes to the CDR have not moved the CDR closer towards this goal. The ABA recommends pausing any changes to the CDR that are directed towards meeting this goal.

- This will enable all participants to focus on implementing changes that either improve the cyber and data security landscape of the CDR or enhance the present customer experience within the CDR. It would also ensure that all proposed changes are strictly focused on making the CDR a viable alternative to screen scraping, per the Statutory Review's recommendation. The ABA's parallel CDR submissions provide a series of essential changes necessary to make the CDR a viable alternative.

- After the implementation of these essential changes, the ABA proposes that if the Government agrees that there should be a ban on screen scraping, that the relevant instruments also provide for a government directed plan for the phased retirement of screen-scraping. The ABA recommends the phased retirement be up to 24 months from the effective date. This should allow sufficient time for the migration of existing business processes and unwinding of commercial relationships. The timeframe of 24 months should also involve a staggered migration away from screen-scraping, commencing with the least economically impactful use cases and progressing over the 12-month period to the most economically significant use cases, such as mortgage applications.

Policy Director contact: Nicholas Giurietto

Head of Future Policy

nicholas.giurietto@ausbanking.org.au

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

ABA Submission on Screen Scraping

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on Treasury's consultation on the Screen Scraping – Policy and regulatory implications discussion paper.

When compared to the CDR, screen-scraping (defined as the practice of obtaining user login credentials in order to simulate user interactions so as to access data or initiate actions) intrinsically poses a higher level of cyber security, fraud and scams risk and a lower level of assurance for privacy compliance. The CDR framework is designed to mitigate both these risks. As such, ABA member banks endorse the recommendation from the CDR Statutory Review that screen scraping be banned *where the CDR is a viable alternative.*

Viability: A comparable customer experience

To make the CDR a viable alternative, it needs to offer a comparable customer experience. To date, some of the previously implemented and currently proposed changes to the CDR have not moved the CDR closer towards this goal. The ABA recommends pausing all proposed changes to the CDR to enable all participants to focus on implementing changes that either enhance the cyber and data security landscape of the CDR or improve the customer experience within the CDR. Prioritising these changes to the CDR will expedite progress towards a ban on screen scraping.

Pause non-essential changes

In order to properly focus resources on making the CDR a viable alternative, the ABA recommends pausing all non-essential changes proposed in the parallel consultations on:

- CDR Rules - Expansion to the non-bank lending sector,
- CDR Rules – Consent review,
- Operational enhancements design paper, and
- The DSB's Authentication Uplift

Many of the proposed changes put forward in the parallel consultations carry little connection to either further enhancing security or improving the CDR consumer experience. As such, the ABA strongly recommends that Treasury pause the implementation of all non-essential components that do not make notable contributions to either enhancing cyber/data security or enhancing the consumer experience. For the avoidance of doubt, the CDR offers a safer alternative to screen scraping but further enhancing the security landscape of the CDR falls into the category of 'essential' changes given the evolving nature of cyber/data security risks.

Two recent examples of non-essential changes are the DSBs considerations for tightening a 'Non-Functional Requirement' response time on requests from Accredited Data Recipients (ADRs) to 1 second and including non-digitised Pass Book accounts on the list of products for inclusion on the CDR. Another example of a non-essential change in the parallel Operational enhancements' consultation considered the possibility of consumer eligibility being extended to data holders operating multiple brands. This is despite such a proposed change being a departure from how consumers currently engage with multiple brands and the significant technological, data segregation and contractual implications. The above changes do not enhance data security or significantly enhance the consumer experience – rather they misdirect valuable resources towards changes which do little to make the CDR more viable. They also divert an entity's focus and resources on

CDR innovation and developing use cases to increase uptake of the CDR. Changes that deliver the highest value to the consumer and return on CDR policy objectives should be prioritised.

Implement essential changes: Enhancing security and offering a comparable customer experience

Pausing non-essential changes would enable entities to concentrate resources on making the CDR a viable alternative to screen scraping and accelerating consumer uptake. The ABA submissions on the parallel consultations (in addition to this submission) as the recommendations put forward are considered by the ABA as important precursors to the viability of the CDR. The recommendations focus on changes that either enhance data/cyber security or deliver an improved customer experience to facilitate increased adoption.

By way of an example, one of the ABA's recommendations put forward in the parallel Consent review submission involved the implementation of enhanced consent flows resulting in an observable improvement in the CDR customer experience and reduced customer drop-outs. This is considered an essential change as it makes a notable contribution to improving the customer experience and therefore the viability of the CDR. Another notable example is the ABA's recommendation to implement FAPI 2.0 specifications. This is considered an essential change as it will significantly uplift the cyber and data ecosystem of the CDR – a ubiquitous consideration of the CDR given the evolving nature of cyber/data security risks.

Once implemented, changes similar to, and including, the examples outlined above will make the CDR a viable alternative to screen scraping as it will offer a comparable customer experience. Additionally, the changes will further enhance the security of the CDR ecosystem, making it even safer than it already is when compared to screen scraping. The Government will then be able to consider a ban on screen scraping and a corresponding retirement plan.

Proposed Government retirement plan

The ABA recommends that any Government directed retirement plan ensures that when the CDR is determined to be a viable alternative to screen scraping, there is a smooth transition to the CDR that avoids disruptions to economically significant customer use cases.

Phased migration: a risk-based approach

It must be acknowledged that, despite its limitations, screen-scraping is currently utilised by some banks to effectively and efficiently support a number of economically significant customer use cases such as the provision of transactional information to support loan credit decisions. Any prohibition of screen-scraping must allow both enough time for the unwinding of existing business processes and commercial relationships as well as ensure that the customer experience utilising CDR is as nearly-as-possible equivalent.

If the Government elects to ban screen scraping, the ABA proposes a Government directed retirement plan of up to 24 months from the effective date. This should allow sufficient time for the migration of existing business processes and unwinding of commercial relationships. The timeframe of 24 months should also involve a staggered migration away from screen-scraping, commencing with the least economically impactful use cases and progressing over the 12-month period to the most economically significant use cases, such as mortgage applications.

Australian Banking Association

Responses to Detailed Consultation Questions

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

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?

There are many different use cases and individual implementations of screen scraping with divergent characteristics, but one example is banking data for loan assessment purposes.

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?

There are many different use cases and individual implementations of screen scraping with divergent characteristics, so it is not possible to generalise. But for some banks, this typically involves providing the customer with terms and conditions and disclosures at the point of them supplying their credentials so that they are making an informed choice as to whether to proceed.

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?

There are many different use cases and individual implementations of screen scraping with divergent characteristics, so it is not possible to generalise.

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

Some banks acting as an ADR equivalent utilise screen scraping for data collection activities underpinning key customer processes such as credit applications. Whilst other banks elect not to use screen scraping at all.

Banks do not support the use of screen-scraping for action initiation.

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

It is important to acknowledge that, despite its limitations, screen-scraping is currently utilised to effectively and efficiently support a number of economically significant customer use cases such as the provision of transactional information to support loan credit decisions. For some, screen scraping provides some benefits, including a convenient and relatively frictionless option to data sharing.

Despite this, screen-scraping creates a number of direct risks to consumers as well as undermining the integrity of cyber security protections:

Screen-scraping normalises poor consumer behaviour that increases vulnerability to fraud and scams.

The practice of consumers sharing login and password details 'trains' consumers to accept that this is a normal business practice and can erode the normal vigilance that would otherwise help protect them scams and fraud. The clear education message to "never share your login or password details" is undermined by the presence of screen-scraping solutions.

Screen-scraping undermines bank fraud protection controls.

It can be difficult for a bank to distinguish between the genuine activity of a customer and automated interactions utilising credentials shared with an organisation utilising screen-scraping. This can make it more difficult to 'tune' biometric fraud controls based on customer interactions to successfully distinguish between legitimate customer activity and potentially fraudulent activity resulting in the inconvenience of false positives or, worse, a delay in identifying a data breach.

Screen-scraping could make it more difficult to identify the source of a data breach.

In the event of a data breach, the availability of screen-scraping can sometimes make it more difficult to identify the source the breach – was it through a customer interaction or compromise of a screen-scraping solution? – and thus slow the response time.

Screen-scraping undermines informed customer consent

Some providers have attempted to implement protections against entities accessing data beyond the scope of the customer's intention. However, a customer providing login and password credentials to a screen-scraping organisation essentially permits 'all you can eat' access to their account and could be exploited to access information or authorise actions well beyond the scope of the customer's intent. Similarly, screen-scraping presents an opportunity for unscrupulous organisations to circumvent the consent controls built into CDR.

Screen-scraping poses a systemic cyber security risk

Given the common customer practice of re-using passwords across different services and service providers, a compromise of login and password credentials held by a screen-scraping organisation could facilitate multiple simultaneous data breaches. A worst-case scenario would be a hack resulting in compromise of credentials used for a substantial number of both bank and telecommunications services which would undermine 2FA authorisation processes. However, the ABA notes that banks utilising screen scraping when acting as an ADR equivalent undertake significant due diligence efforts to ensure that the provider of screen scraping services appropriately mitigates cyber security risks.

Screen-scraping poses broader privacy risks

Risks associated with screen-scraping may extend beyond consumers sharing log in credentials. For example, US start up ClearView was found to have breached the Australian Privacy Principles by using screen-scraping to scan customer images on websites such as Facebook and LinkedIn to propose identity matches for images of individuals. But the ABA notes the discussion paper's stated focus on screen scraping in the form of sharing log in details.

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

Research by an ABA member bank has revealed a correlation between the use of screen scraping services and the customer's propensity to fall victim of scams or fraud. This does not necessarily provide evidence of causation, but it is at least a credible hypothesis that (as noted above) screen-scraping normalises poor credential security behaviours that contribute to greater vulnerability to fraud and scams.

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?

Bank identity verification protocols and cyber security controls may identify transactions, including when a transaction is initiated via an unusual IP address, that are potentially conducted by a screen scraping service. The bank response to any such transaction will be managed according to its individual risk management framework. In some cases, customer notifications of potential screen-scraping transactions have been trialled in order to confirm customer consent.

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

Banks utilising screen scraping when acting as an ADR equivalent undertake significant due diligence efforts to ensure that the provider of screen scraping services appropriately mitigates cyber security risks. For some banks, this includes appropriate monitoring, auditing and risk assessments for the risk associated with screen scraping.

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

Clear alignment of the Government's digital identity strategy with CDR processes will help ensure an optimum user experience and minimise the risk of duplicative investments to enhance CDR functionality.

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

Recently, the US's Consumer Financial Protection Bureau (CFPB) has proposed a Personal Financial Data Rights rule (**PFDR Rule**) to move away from screen scraping and

towards Open Banking. The PFDR Rule would oblige companies to share data held on a consumer at the consumer's direction. It aims to increase competition, improve financial products and services and provide consumers with greater control over their data. Like Australia's CDR, the PFDR Rule proposed to implement it in phases, starting with the larger providers.

The ABA recommends considering some of the principles espoused in the proposed PFDR Rule, particularly the principles around the 'Standard-Setting Body'. For example, the principle of due process refers to the need for adequate notice for standards development and sufficient time to review drafts – principles that are not always consistently applied in the implementation of new CDR Rules and standards in Australia.

8. 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?

Unlike screen scraping, CDR is currently limited to industry sector coverage. So, many data sets are currently accessed through screen scraping which cannot be accessed through the CDR. There are certain types of data that the financial service sector would most significantly benefit from having access to through the CDR such as superannuation, and insurance data. Access to these through the CDR would significantly drive uptake of the CDR as they relate to lending applications, one of the most common use cases for screen scraping. It would also enable innovation into additional use cases, potentially not yet envisioned or leveraged through screen scraping. However, the ABA reiterates the importance of the CDR being made a viable alternative first.

Should an ADR identify a relevant data element that cannot currently be obtained under CDR Rules they should make the policy case for the inclusion of that additional data in the already comprehensive CDR data catalogue.

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?

One restriction related to the ability of AFSL entities to participate in the CDR and use data is the absence of a streamlined accreditation process akin to the streamlined process for ADIs. The ABA endorses the Financial Services Council (FSC) submission point on streamlining the accreditation process for FSC members holding Australian Financial Services Licenses (AFSL). The absence of a streamlined approach for AFSL holders unnecessarily limits the ability of these entities to become accredited data recipients and contribute to uptake of the CDR. Both ADIs and are FSC members holding an AFSL are subject to APRA's prudential standard CPS234: information security standard as well as the new CPS230: operational resilience. Both require a high standard of data and cyber security. Therefore, the ABA supports the FSC's recommendation to appropriately extend the streamlined process of becoming an accredited data recipient to other entities, particularly those who hold an AFSL.

A further restriction is that certain CDR rules do not currently offer a viable pathway for Authorised Deposit- taking Institutions (ADIs) to participate as Accredited Data Recipients (ADRs) for lending use cases. For ADRs that are also ADIs, the requirement to treat data received via the CDR differently to the data received through conventional means serves as an inhibitor to the development of use cases. This results in lenders modifying well established downstream systems, processes and policies to meet the current rules.

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

No such requirements have been identified at this time.

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

Presently, some consumers appear to prefer using screen scraping as a similar experience is not currently possible under the CDR given the frictions imposed around consent. One member bank notes that internal data indicates that uptake of the CDR has been very low amongst business customers. This is despite it being very common for business customers to use non-CDR data sharing options. Understanding the drivers of low adoption (consent friction being one of them) will be key to increasing adoption.

In order for CDR to be a viable alternative to screen scraping it needs to offer a comparable customer experience.

The ABA strongly recommends pausing all non-essential changes to enable participants to focus on implementing changes that either improve the cyber and data security landscape of the CDR or enhance the present customer experience within the CDR. Some recent examples of non-essential changes include:

- The DSB's considerations for tightening a 'Non-Functional Requirement' response time on requests from Accredited Data Recipients (ADRs) to 1 second.
- The DSB's consideration for including non-digitised Pass Book accounts on the list of products for inclusion on the CDR.
- The Operational Enhancements design paper considered the possibility of consumer eligibility being extended to data holders operating multiple brands. This is despite such a proposed change being a departure from how consumers currently engage with multiple brands and the significant technological, data segregation and contractual implications.

None of the above changes increase data security or significantly enhance the consumer experience – rather they misdirect valuable resources towards changes which do little to make the CDR more viable.

To understand what these essential changes are, the ABA recommends reviewing our submissions on the parallel consultations (in addition to this submission) as the recommendations put forward are considered by the ABA as important precursors to the viability of the CDR. The recommendations focus on changes that either increase data security or deliver an improved customer experience to facilitate increased adoption. Two

examples of ABA recommendations in parallel consultations which are considered essential and require adjustment include:

- enhancing consent flows resulting in an observed improvement in the CDR customer experience and reduced customer drop-outs; and
- implementing FAPI 2.0 specifications to significantly uplift the cyber and data ecosystem of the CDR and enable purpose-based consents.

Beyond viability, the ABA also suggests that the Government increase public education and awareness about the CDR to drive consumer uptake.

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?

In order for CDR to be a viable alternative to screen scraping it needs to a comparable customer experience.

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

The ABA broadly endorses the recommendation from the CDR Statutory Review that screen scraping be banned *where the CDR is a viable alternative*. However, presently the CDR is not considered a viable alternative to screen scraping. To make the CDR a viable alternative, it needs to offer a comparable customer experience. To date, many of the previously implemented and currently proposed changes to the CDR have not moved the CDR closer towards this goal. The ABA recommends pausing any changes to the CDR that are directed towards meeting this goal. This will enable entities to focus on essential changes to the CDR that make notable contributions to enhancing cyber or data security or improving the consumer experience.

After the implementation of these essential changes, the ABA proposes that if the Government agrees that there should be a ban on screen scraping, that the relevant instruments also provide for a government directed plan for the phased retirement of screen-scraping.

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

Only after the delivery of the required capability to ensure that CDR is a viable alternative for screen-scraping, does the ABA propose a timeframe for retirement of screen scraping. Should the Government elect to ban screen scraping, the ABA proposes that industry would requires up to 24 months from the effective date. This should allow sufficient time for the migration of existing business processes and unwinding of commercial relationships. The timeframe of 24 months should also involve a staggered migration away from screen-scraping, commencing with the least economically impactful use cases and progressing

over the 12-month period to the most economically significant use cases, such as mortgage applications.