Commonwealth Bank

Screen Scraping – policy and regulatory implications

Response to Discussion Paper

Executive Summary

CBA welcomes the opportunity to contribute to Treasury's consultation on the policy and regulatory implications from screen scraping.

In an increasingly digital world, the safety and security of our customers' data is paramount. CBA has long been concerned with screen scraping practices which introduce a multitude of risks to consumers and businesses in relation to their data.

CBA believes that screen scraping should be prohibited for the following reasons:

- **There is a safer alternative:** CBA believes the Consumer Data Right ("CDR") is a safer and preferable alternative to screen scraping. CBA, along with many other financial institutions, has invested significantly in the development of the CDR which is a more secure and effective way for consumers to share their data. The CDR puts consumers in control, giving them the choice of what data they want to share with other accredited institutions and for how long. By comparison, screen scraping provides unrestricted access to customer bank accounts and offers few controls to manage consumer data security and privacy.
- **Driving adoption and innovation with the CDR:** Banning screen scraping will ensure consumers are migrated to CDR, a much safer way of sharing their data. Driving increased engagement with CDR will encourage the market to innovate using the CDR platform driving further uptake and engagement. Banning screen scraping will also provide the context to support education campaigns to Australians to promote safer data sharing.
- **Helping reduce scams and fraud:** Prohibiting screen scraping will allow both banks and the Government to provide Australians a simpler message that they should not share their banking password under any circumstances and to use CDR instead. It will also reduce the risk that consumers may lose protections under the ePayments code.

CBA's view aligns with the recent Government reviews, such as Future Directions for the Consumer Data Right ("Farrell Review", 2020) and the Statutory Review of the CDR ("Statutory Review", 2022).

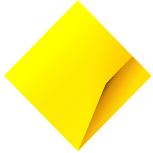
CBA's position remains that screen scraping should be phased out, starting with more mature CDR sectors, such as banking, following a 12-month notice period. A wider ban in all other sectors should follow with a sufficient notice period. Further, CBA encourages that a ban on screen scraping should precede the commencement of action initiation and follow the implementation approach taken for major and non-major banks within the CDR.

1. How is Screen scraping currently used?

CBA does not currently use screen scraping or have third party arrangements with companies that deploy screen scraping technology as defined by the discussion paper, being the form of screen scraping that involves consumers sharing their personal login details with third parties, such as internet banking login details.[1] CBA notes that the common use cases of screen scraping are well summarised by the discussion paper.

The Statutory Review determined that there is currently significant use of screen scraping across the economy.[2] In banking and financial services, screen scraping technology typically provides access to a customer's bank account using the customer login credentials. Those credentials may be stored by the third party, which means they can scrape data from the bank account and use this information just like the customer would. Everything a customer can see or do in their online banking can be done by the third

[1] https://treasury.gov.au/sites/default/files/2023-08/c2023-436961-dp.pdf (page 4)
[2] https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf



party. As this submission emphasises, screen scraping processes raise significant security concerns as consumers may not be able to guarantee that their credentials will be used for express purposes that they are provided, and there can be ambiguity around how consumers can rescind consent once credentials are provided.[3] Customers may end up sharing their credentials with malicious actors and provide bank account access they never intended. As others have pointed out, from a technical perspective, screen scraping is a brittle and insecure method of data collection frequently prone to errors.[4] Specifically, screen scraping methods are based on navigating whole web pages, requiring a lot of data to be downloaded and processed to pinpoint a subset of sought-after information. Screen scraping is thus much slower than APIs, which establish a direct connection between a data holder and a data recipient.

While screen scraping has predominately captured banking and financial services data, there are broader applications of screen scraping that present consumer risk. The Office of Australian the Information Commissioner (OAIC) has reported on the impacts of mass data scraping from social media applications and other websites that host publicly accessible personal information. [5] The use of screen scraping practices in conjunction with social media platforms raises particular concern in a high scams environment where vulnerable customers are often susceptible to scams. Social media platforms are now commonplace for attacks, with personal data easily accessible and scammers readily able to create sponsored ads. The ACCC's Scamwatch reports that Australians lost $80.2 million to social media scams last year, an increase of 43% on the year before.[6]

2. What are the risks of Screen scraping?

Risks to Consumers

The risks to consumers from screen scraping are well established in the discussion paper. CBA makes the following commentary on the risks raised:

- **Counters online security best practices at the consumer level** – Asking consumers to engage in any practice in which they disclose login and password information to third parties runs counter to IT security best practices. The OAIC's latest Notifiable Data Breaches Report: January to June 2023 shows that close to half of data breaches during the period where either compromised or stolen credentials (method unknown) or phishing attacks involving compromised credentials.[7] Against a backdrop of heightened security awareness following recent large-scale data breaches in Australia, it may be difficult for some consumers to navigate what actions are right for them if they are given mixed messages about the risks associated with sharing their login details. Simply offering credentials to third parties compromises safety as often consumers share credentials in an unencrypted format and frequently use the same passwords to access a wide variety of online accounts.[8]
- **Counters good online practices at the enterprise and sector level** – In financial services, APRA's CPS 234 drives significant investment in the Information Security for regulated entities and yet the use of screen scraping by financial service organisations with poor Information Security protocols, which are not regulated by APRA, provide a weak link in the cyber ecosystem which can be exploited by criminals.
- **Fraud** - The Basel Committee on Banking Supervision has previously stated screen scraping can "undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and

[3] https://www.oaic.gov.au/newsroom/clearview-ai-breached-australians-privacy
[4] http://www5.austlii.edu.au/au/journals/UNSWLRS/2023/3.pdf
[5] https://www.oaic.gov.au/newsroom/global-expectations-of-social-media-platforms-and-other-sites-to-safeguard-against-unlawful-data-scraping
[6] https://www.scamwatch.gov.au/types-of-scams/social-media-scams
[7] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023
[8] CyberCX (2019), Submission to the Senate Select Committee on Financial Technology and Regulatory Technology, Submission 61, accessed on 5 October 2023

extracting sensitive data".[9] CBA's Fraud Analytics team has analysed data of customers' log-ins via screen scraping IP and determines that customers with aggregator activity are 46% more likely to experience fraud than an 'average' customer. Whilst the study does not attribute cause for the statistical relationship between screen scraping and fraud, it does demonstrate a correlation between the unsafe banking practice of customers who share log-ons and password credentials with third parties and increased fraud.

- **Limited regulation and effect on vulnerable customers** – As screen scraping is not currently regulated, consumers may not always understand when they are using services that rely on screen scraping nor the associated risks. Because screen scraping involves consumers providing account login details, they may also have little control over what specific data and access the third party may have and how the consumer can end the arrangement. Jevglevskaja and Buckley (2023) have written about the dangers of screen scraping against vulnerable customers as it facilitates predatory lending.[10]
- **Loss of consumer protections under ePayments Code** – Consumers who share their login details through screen scraping may lose protections available to them under the ePayments Code to be indemnified for losses caused by unauthorised transactions. ASIC noted in its latest review of the ePayments Code that consumers use screen scrapers at their own risk, should it amount to 'disclosure' of a passcode.
- **Disclosure risks in the event of a data breach** – If any screen scraping providers experience data breaches in the future, large volumes of banking login details or passwords could be exposed and compromise consumer trust online, and create detrimental impacts to the digital economy. This could give rise to 'credential stuffing', a type of cyber incident in which a threat actor collects and uses compromised credentials, often obtained in other data breach incidents, to access other systems and accounts without authorisation. Scraped identity and contact information posted on 'hacking forums' may also be used by malicious actors in targeted social engineering or phishing attacks. [11]

Given the risks, allowing screen scraping practices to persist contravenes current advice provided by the Australian Government and policy priorities. For example:

- The Government's current 2023-2030 Cyber Strategy consultation process prioritises efforts to build greater community awareness in the practical steps that consumers and businesses can take to improve their cyber resilience.[12]
- The ACCC's National Anti-Scam Centre and Scamwatch website advises consumers not to share login details.[13]
- MyGov's Terms of Use outlines that only users are responsible for their MyGov account and that users must not share credentials[14]; and
- The Australian Cyber Security Centre's 'Guidelines for System Hardening' details guidance for system hardening including controls to protect credentials.[15]

CBA's action to prevent screen scraping

[9] Basel Committee on Banking Competition, Report on open banking and application programming interfaces, November 2019
[10] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4382528
[11] https://www.oaic.gov.au/newsroom/global-expectations-of-social-media-platforms-and-other-sites-to-safeguard-against-unlawful-data-scraping
[12] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper
[13] https://www.scamwatch.gov.au/protect-yourself/ways-to-spot-and-avoid-scams
[14] https://my.gov.au/en/about/terms#:~:text=You%20are%20responsible%20for%20your,these%20details%20with%20anyone%20else.
[15] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

CBA is aware of businesses that screen scrape data from our consumer facing online platforms despite it being in breach of our customer terms and conditions. Rather than blocking access from businesses that use screen-scraping, CBA notifies customers where we observe screen scraping activity on their account. In these circumstances, we warn our customers of the potential risk and inform them on steps they can take to protect their security and privacy online.

These communications are consistent with the annual notifications we are required to provide under the ePayments Code. As a subscriber to the ePayments Code, we are required at least annually to provide a clear, prominent notice summarising passcode security guidelines (clause 8.1). These guidelines must be consistent with the passcode security provisions (clause 12) of the Code, which, amongst other things, include clause 12.2(a), which provides that users must not voluntarily disclose passcodes to anyone, including a family member or friend.

3. Reforms and Legal Frameworks related to the screen scraping

3.1 Reform and Legal Frameworks

Buy-Now-Pay-Later

In relation to currently proposed responsible lending reforms to give effect to the Government's intention to regulate the Buy Now Pay Later, CBA does not endorse screen scraping being enabled to facilitate responsible lending processes. CBA has advocated that BNPL providers should take reasonable steps to assess whether a product is right for a consumer, including by performing comprehensive credit checks.[16] Greater cross-sectoral designation and adoption of uplifted security profiles such as FAPI 2.0 will promote more secure and persuasive use cases developing from the CDR.

The Privacy Act

Regarding the Australian Government's recent Review of the *Privacy Act* and subsequent response released in September 2023, CBA notes the Government's agreement-in-principle for reforms concerning 'fair and reasonable information handling'. While noting the Attorney-General's response that entities will still be permitted to collect personal information, they also state that

> the fair and reasonable test will ensure that the impact on individuals resulting from an entity's handling of personal information and the public interest in protecting privacy are considered alongside the entity's interest in carrying out its activities or functions. [17]

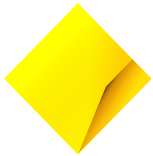
This new requirement promises to help protect individuals when their personal information is used in complex data processing activities, which have emerged through technological advancement, such as screen scraping. CBA supported this recommendation though cautioned that

> given that the proposed legislated factors read ambiguously on their own, and given that the test will regulate many different types of data handling practices, there will be inconsistencies when applying across the economy.[18]

To support implementation, CBA welcomes OAIC guidance and enforcement through determinations relying on judicial consideration to provide clarity on the fair and reasonable test over time. This is outlined in the Government's response to the Privacy Act review.[19]

---

[16] https://treasury.gov.au/sites/default/files/2023-02/c2022-338372-cba.pdf
[17] https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF (page 8)
[18] https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF (page 8)
[19] https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF



Other adjacent initiatives

CBA welcomes additional initiatives underway to secure Australian's data in the digital economy, such as work to combat scams and fraud, update the 2023-2030 Cyber security strategy, expansion of the Digital Identity framework, and mandating the ePayments code.

3.2 International Developments

Screen scraping is also an issue in other similar economies around the world with Government's responding to the need to remove the risks that this activity creates. For example those that are noted in the discussion paper in relation to the European Union's revised Payment Services Directive (known as PSD2) and under the UK's Open Banking framework.

CBA notes the US Consumer Financial Protection Bureau (CFPB) has extensively examined screen scraping dating back to 2017 where it was acknowledged that there is heightened sensitivity around consumers sharing or authorising access to login credentials.[20] Speaking to the benefits of open banking, CFPB Director Rohit Chopra has remarked that

> "there will be better security of personal financial data. One reason that the current ecosystem is unstable is that many companies currently access consumer data through activities like screen scraping. However, such methods are not secure, and they are likely not sustainable, especially as data security standards potentially evolve to a point that such activities may become blocked".[21]

On 19 October 2023, the CFPB proposed a *Personal Financial Data Rights* rule that would accelerate a shift toward open banking, where consumers would have control over data about their financial lives and would gain new protections against companies misusing their data. According to the CFPS, the proposed rule would prevent risky data collection practices, such as screen scraping. The CFPB noted that prior feedback received through public comments and stakeholder outreach, there is nearly universal consensus that developer interfaces should supplant screen scraping. The CFPB are currently consulting on its proposal through to 29 December 2023.[22]

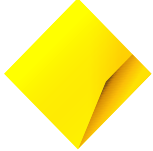
4. The Consumer Data Right

CBA notes recommendation 2.1 of the Statutory Review which outlined that "screen scraping should be banned in the near future in sectors where the CDR is a viable alternative" and welcomes the Government signalling when and how the implementation of a ban on screen scraping would take effect.

As a starting point regarding suggestions on how to improve the CDR framework so that it becomes a more viable alternative to screen scraping, CBA acknowledges the issues raised by the Statutory Review, and substantial work that has commenced since to improve the performance and functionality of the CDR. These include:

- **Data quality** –CBA does not see data quality as the primary issue hindering CDR take up. The ACCC have since conducted reported on Data Quality in the CDR and while there are clear areas for improvement, found that the quality of consumer data is generally sufficient to support the delivery of CDR products and services.[23] Ensuring a strong regulatory presence, clarifying obligations to improve data quality, and improve consultation process which the CDR regulators have committed to will see data quality in the CDR ecosystem further improve.

[20] Microsoft Word - cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights clean (consumerfinance.gov)
[21] https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/
[22] CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking | Consumer Financial Protection Bureau (consumerfinance.gov)
[23] https://www.accc.gov.au/system/files/Data-Quality-in-the-Consumer-Data-Right-Findings-from-Stakeholder-Consultation.pdf



- **Complexity of the system** – the Statutory Review found that CDR rules and standards were overly complex and compliance focused which has prevented participants from developing new products and services. CBA agrees that as the CDR matures and stabilises, participants will likely develop the system to increase customer value. In the interim, policy makers should consider changes to the volume and frequency of rule changes which add complexity to the framework, increase compliance costs, and constrain innovation.
- **Lack of awareness** – the priority around increasing consumer awareness of the CDR has been well documented in past treasury consultations. Of course, consumer awareness of the CDR will only emerge once persuasive use cases are in market. CBA believes that allowing screen scraping to continue alongside the CDR will result in perpetual 'dual schemes' being in operation, to the detriment of consumers as well as take up and participation in the broader CDR regime. Jevglevskaja and Buckley (2023) have shown that following tighter restrictions on screen scraping in the UK coming into effect, the UK saw a surge in API calls through their open banking framework: from 12 million a day in February 2020 to 24 million a day a year later, and up to 31 million a day in February 2022, or 860 million calls for the month. The UK experience in particular shows that even partial phasing out of screen scraping can act as a spur to ensure that APIs perform well and the ecosystem grows rapidly and with due attention to data quality.[24] In time, designation of more data sets will drive consumer awareness and use cases.

In relation to when Government might determine that the CDR is a viable alternative, CBA suggests that it depends on the maturity of the sector within the CDR framework. For example, banking participants would be able to move relatively quickly compared to the energy sector and non-designated sectors. It follows that screen scraping's prohibition could be phased on a sectoral basis and come into effect after a 12-month notification period to enable businesses using screen scraping time to transition and ensure data holders can support the additional volume of API calls.

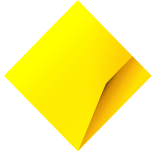
CBA notes there are various accreditation models under the CDR that organisations transitioning away Screen Scraping business models can adopt, which facilitate innovation and competition. As the CDR ecosystem has matured, software and platform service providers have grown and enabled modularised CDR solutions, without requiring a ground-up build. This enables benefits such as higher security standards, greater speed to market through streamlined pre-requisites for participation, and promotion of CDR ecosystem growth which supports the development of Australian businesses.

In addition to payment system reforms and licensing CBA recommends uplifts in PayTo standards, regarding liability and capital requirements, are executed and a screen scraping prohibition should precede the commencement of action initiation within the CDR. Restricting screen scraping prior to enabling write access functionality was a rationale followed by the European Union when the Payment Service Directive (PSD2) prohibited third party payment service providers from screen scraping in advance of banks putting in place a communication channel that allows TPPs to access the data that they need in accordance with PSD2.[25] CBA maintains that combining screen scraping with write access functionality could introduce significant new risks into the CDR framework in relation to fraud. For example, without proper safeguards around payment initiation, a third party could act in malevolent ways contrary to the consumer's express instructions.

Finally, restrictions and enforcement action should be applied to the source initiating the screen scraping request. CBA urges that there should be no requirement under the legislation for data holders to apply restrictions nor should there be penalties for blocking screen scraping activity when its identified.

---

[24] http://www5.austlii.edu.au/au/journals/UNSWLRS/2023/3.pdf
[25] https://ec.europa.eu/commission/presscorner/detail/pl/MEMO_17_4961



5. Conclusion

Proposals for a prohibition on screen scraping are consistent with CBA's past submissions and findings from the Future Directions for the Consumer Data Right ("Farrell Review", 2020) and the Statutory Review of the CDR ("Statutory Review", 2022).

The risks from screen scraping are well established in the discussion paper and elaborated on in this submission. Following high-profile data breaches and emergence of a high scams and fraud environment, addressing these risks should be a Government priority to protect against consumer harm and strengthen good cyber practices. A lack of clear action on screen scraping embeds policy inertia that will not serve the Australian digital economy in the longer term.

CBA welcomes a holistic, cross-government, approach to prohibiting screen scraping. A clear signal from Government through a legislated ban will ensure consumers are better protected, and incentivise businesses to more quickly transition to using safer means such as the CDR.