Consumer Data Right Policy and Engagement Branch
Market Conduct and Digital Division
The Treasury
Langton Crescent
PARKES ACT 2600
By email: data@treasury.gov.au

25 October 2023

Harmful data practices should be minimised in principle and must be eliminated where CDR is a viable alternative[*]

Submission to the consultation 'Screen Scraping – Policy and Regulatory Implications'

Dr Anton Didenko
Senior Lecturer, Faculty of Law and Justice
UNSW Sydney, Australia
anton.didenko@unsw.edu.au

The commitment of the Australian government to tackle the risks of sharing customer data generated by screen-scraping and adjust the regulatory framework accordingly following public consultation is commendable and deserves recognition.

This submission supports the legal prohibition of screen-scraping where the Consumer Data Right is a viable alternative.

More specifically, it is submitted that:

- as a data sharing practice, screen-scraping facilitates breaches of security of consumer data *by design*;

---

* This submission is based on the author's publications: Anton Didenko, 'Australia's Consumer Data Right and Its Implications for Consumer Trust' (2024, forthcoming) 50(1) *Monash University Law Review* <https://ssrn.com/abstract=4543464>; Anton Didenko, 'New Ways to Reinforce Consumer Trust in Australia's Consumer Data Right' (2024, forthcoming) 50(1) *Monash University Law Review* <https://ssrn.com/abstract=4543505>. The above publications were funded by the Australian Government through the Australian Research Council (project FL200100007 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks'). The views expressed herein are those of the author and are not necessarily those of the Australian Government or Australian Research Council.

- Australian law is unforgiving towards consumers who condone screen-scraping and suffer losses as a result;

- the risks of screen-scraping are widely recognised overseas;

- screen-scraping generates perverse incentives that may inhibit the development of the Consumer Data Right;

- if adopted, the prohibition on screen-scraping should avoid ambiguous criteria.

This brief submission outlines the key arguments. Additional analysis is available in my forthcoming publications in the *Monash University Law Review*:

- Anton Didenko, 'Australia's Consumer Data Right and Its Implications for Consumer Trust' (2024, forthcoming) 50(1) *Monash University Law Review*. Link: SSRN;

- Anton Didenko, 'New Ways to Reinforce Consumer Trust in Australia's Consumer Data Right' (2024, forthcoming) 50(1) *Monash University Law Review*. Link: SSRN.

1. Background

Australia's Consumer Data Right ('CDR') is a world-leading example of a cross-sectoral framework to facilitate the secure and responsible sharing of consumer data. Its competition-promoting objectives hold the key to unlocking the potential of wider sharing of consumer data, as long as the relevant risks are adequately managed. The CDR relies on, and helps to build and reinforce, consumer trust. In so doing, it offers a viable alternative to unsafe data sharing practices like screen-scraping.

2. Arguments against screen-scraping

Despite offering a sophisticated toolkit for the sharing of consumer data across the economy, the CDR framework remains merely an *alternative* that consumers may elect to use or ignore. Other data sharing practices are not prohibited – on the assumption that the CDR will be attractive enough to sway consumers. Screen-scraping that involves disclosing internet banking access credentials to a third party is an example of alternative practices of sharing consumer data that remains widely available. There are several important issues with this status quo.

2.1. Screen-scraping is risky by design

There are no agreed standards for 'safe' screen-scraping – perhaps because it is difficult to develop standards for the *use* of something that one should *not possess* in the first place: it is standard practice for issuers of login credentials to prohibit and discourage their sharing with any third party.

Even when done with a consumer's consent, 'legal screen scraping can be hard to distinguish from illegal automation, like malicious bots or credential stuffing'[1] – which makes monitoring and enforcement of cyber incidents particularly problematic. According to some commentators, financial institutions have resorted to whitelisting known aggregator IP addresses 'as the aggregators simply cause too much traffic for the fraud prevention teams to effectively investigate'.[2] This leaves major gaps in information security that could only be explained by reasons of convenience: in some cases, 'aggregators represent up to 25% of financial institutions' total traffic – something that would take fraud prevention teams [years] to analyze manually if not safe-listed by their bot detection tools'.[3]

2.2. Australian law is unforgiving towards consumers who condone screen-scraping and suffer losses as a result

Unless screen-scraping becomes a regulated activity, consumers who disregard the instructions of the issuer of their login credentials remain exposed to significant *legal* risks since by disclosing those credentials consumers breach their customer duties. Indeed, consumers

[1] Olov Renberg, 'Fintech Aggregators and Open Banking: Service Enablers or an Unfortunate Backdoor for Fraud?', Security Boulevard (Web Page, 8 December 2021) <https://securityboulevard.com/2021/12/fintech-aggregators-and-open-banking-service-enablers-or-an-unfortunate-backdoor-for-fraud/>.

[2] Ibid.

[3] Ibid.

resorting to screen-scraping find themselves in breach of their financial institution's terms and conditions.[4]

Furthermore, ASIC's ePayments Code clearly states that users 'must not…voluntarily disclose one or more passcodes to *anyone*, including a family member or friend'.[5] More recently, in a public consultation concerning the revised ePayments Code ASIC reiterated its 'let consumer beware' approach:

> Our proposal does not prevent consumers from using screen scraping services. It does aim to clarify the existing position that a *consumer does so at their own risk* that, should the inputting of their internet banking credentials for this purpose amount to 'disclosure' and contribute to an unauthorised transaction, they may be liable for the resulting financial loss.[6]

Australian banking case law is equally unforgiving towards customers who ignore to take simple precautions against fraud:

> No one can be certain of preventing forgery, but it is a very simple thing in drawing a cheque to take reasonable and ordinary precautions against forgery. If owing to the neglect of such precautions it is put into the power of any dishonest person to increase the amount by forgery, the customer must bear the loss as between himself and the banker.[7]

While the Macmillan duty is limited to cheques, it clearly demonstrates the *expectation* that bank *customers cannot act irresponsibly* (such as by signing a cheque without stating the sum in words) and then rely on the law to intervene and protect them. By the same logic, it seems implausible that common law will interfere to protect customers who *willingly* enable a third party to take control of their online banking credentials.

It follows that while consumers are free to trust companies offering screen-scraping services, they are likely to remain unprotected if those companies prove to be unworthy of that trust.

2.3. The risks of screen-scraping are widely recognised overseas

The risks of screen-scraping are not unique to Australia and have been acknowledged internationally:

> The practice of using login credentials for screen-scraping poses significant security risks, which have been recognized for nearly two decades. Screen-scraping *increases cybersecurity and fraud risks* as consumers provide their login credentials to access fintech applications. During outreach meetings with Treasury, there was *universal agreement* among financial services companies, data

---

[4] Reserve Bank of Australia, Submission to Treasury, *Inquiry into Future Directions for the Consumer Data Right - Issues Paper* (23 April 2020) 3 <https://treasury.gov.au/sites/default/files/2020-07/rba.pdf>.

[5] Australian Securities and Investments Commission, *ePayments Code* (2 June 2022), cl 12.2(a) (emphasis added).

[6] Australian Securities and Investments Commission, *Report 718 – Response to Submissions on CP 341 Review of the ePayments Code: Further Consultation* (March 2022) 37.

[7] *London Joint Stock Bank Ltd v Macmillan and Arthur* [1918] AC 777, 811. The so-called Macmillan duty was accepted by Australian courts in *Commonwealth Trading Bank of Australia v Sydney Wide Stores Pty Ltd* (1981) 35 ALR 513.

> aggregators, consumer fintech application providers, consumer advocates, and regulators *that the sharing of login credentials constitutes a highly risky practice*.[8]

Indecisiveness leaves consumers exposed to these risks – as recognised by the United States Department of Treasury:

> As described by one observer, 'the U.S. debate seems stuck at the yet-to-be resolved issue of migrating account aggregators from screen scraping-based to more secure and efficient API-based data-sharing methodologies.' *As long as this impasse remains unresolved, consumers will be caught in the middle*.[9]

Furthermore, the Final Report of the Canadian Government's Advisory Committee on Open Banking treats screen-scraping as a dangerous practice demanding a regulatory response:

> Screen scraping presents real security and liability risks to Canadians as it requires them to share their banking login credentials with third party service providers. As screen scraping proliferates, so too will the associated risks to Canadian consumers and financial institutions.[10]

According to the same report, open banking should be launched with haste '[t]o *eliminate* screen scraping'[11] – not condone it.

2.4. Screen-scraping generates perverse incentives that may inhibit the CDR

Continued co-existence of the CDR alongside screen-scraping creates perverse incentives. Businesses offering data capture services are given no incentive to abandon screen-scraping – just as they are given no incentive to innovate or improve their information security practices.

Indeed, certain stakeholders have argued that ASIC should not interfere with screen-scraping on the grounds that the Consumer Data Right 'is not yet at a stage where it is considered by the industry as a viable alternative to "screen scraping" and other forms of digital data capture of such value as to outweigh the regulatory costs of participating in the CDR framework'.[12]

Even if the CDR does one day become considered by the industry 'as a viable alternative', without regulatory intervention the same businesses will likely opt to retain screen-scraping as a viable *additional* source of valuable consumer data and thus maintain *both* streams of consumer data, as long as this remains technically feasible and profitable.

---

[8] United States Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation* (Report to President Donald J. Trump, July 2018) 34 <https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf> (emphasis added) (citations omitted).

[9] Ibid 27 (emphasis added) (citations omitted).

[10] Advisory Committee on Open Banking, *Final Report* (April 2021) 3 <https://www.canada.ca/content/dam/fin/consultations/2021/acob-ccsbo-eng.pdf>.

[11] Ibid 4 (emphasis added).

[12] ASIC, *Response to Submissions on CP 341 Review of the ePayments Code: Further Consultation* (Report No 718, March 2022) [115] 34.

2.5. CDR as a 'viable' alternative and legal certainty

Prohibition of screen-scraping where the CDR is a 'viable' alternative is a plausible approach. However, its implementation should avoid ambiguous criteria – in order to promote legal certainty. Equally, due to the perverse incentives discussed above, any viability assessment should not measure to what extent the CDR has already displaced screen-scraping in a particular sector: accredited data recipients may choose to maintain both channels of customer data at once, not to mention the difficulties with calculating the opportunity costs of incomplete transition to the CDR due to screen-scraping. Thus, once the Government has fully implemented the CDR in a particular sector, screen-scraping should be 'switched off' at once.

It is worth stressing that the CDR framework has already clearly demonstrated a strong preference for legal certainty. An example is the 'safe harbour' in section 56GC of the *Competition and Consumer Act 2010* (Cth), which protects the service providers from legal risks despite the fact that *consumers end up bearing the residual risks* of that provision. Therefore, it is hoped that in matters that seek to *protect consumers* from harmful data sharing practices, the policy of legal certainty will be pursued with more rigour, not less.