



ASIC
Australian Securities &
Investments Commission

Australian Securities
and Investments Commission

Office address (inc courier deliveries):
Level 5, 100 Market Street,
Sydney NSW 2000

Mail address for Sydney office:
GPO Box 9827,
Brisbane QLD 4001

Tel: +61 1300 935 075

www.asic.gov.au

Claire McKay, A/Assistant Secretary
Consumer Data Right Policy and Engagement Branch
Market Conduct and Digital Division, Markets Group
The Treasury
Langton Crescent
Parkes ACT 2600

By email only: data@treasury.gov.au

24 October 2023

Dear Claire

ASIC submission to the Discussion Paper: Screen scraping – policy and regulatory implications

The Australian Securities and Investments Commission (**ASIC**) welcomes the opportunity to provide a submission to Treasury on the Discussion Paper: Screen scraping – policy and regulatory implications (**Discussion Paper**).

The Discussion Paper seeks views on the recommendation of the [Statutory Review of the Consumer Data Right \(CDR\)](#) that screen scraping be banned where the CDR is a viable alternative. ASIC considers that the CDR is an important Government initiative that will deliver benefits to consumers and drive innovation. ASIC supports the Government's rollout of the scheme.

Summary

As the national regulator for consumer credit, ASIC is aware of the importance of access to consumer data to assist participants in the lending sector to undertake responsible lending assessments and to facilitate competition in the provision of consumer credit.

We understand that some participants in the consumer credit (and financial services) sector are using screen scraping but others are increasingly using the CDR in place of, or in conjunction with, screen scraping.

Having regard to scams and cyber security risks, and the risks of sharing of banking login details in an environment in which consumers increasingly need to be vigilant about their online security, ASIC considers that the consumer protection safeguards built into the CDR make the CDR a preferable framework for consumers to share their data with third parties.

In these circumstances, ASIC supports the Government's consideration of a ban on screen scraping and relying on the CDR framework to maintain the wider benefits associated with access to consumer data, including for participants in the lending sector to undertake responsible lending assessments and to support competition in financial services.

The ePayments Code

ASIC administers the ePayments Code, a code to which most authorised deposit-taking institutions and a small number of other payments service providers voluntarily subscribe. The Code provides important consumer protections in relation to electronic payments, including credit and debit card transactions, online payments, and internet and mobile banking.

In 2022, ASIC completed a review of the ePayments Code that included, among other things, consideration of the appropriateness and relevance of the settings around unauthorised transactions. ASIC received mixed feedback about screen scraping during the review, including:

- consumer groups and the banking industry generally shared a view that it was not appropriate for consumers to be sharing login details with third party service providers when the CDR framework being rolled out by the banking industry was an efficient and secure way for consumers to share data; and
- some respondents in the digital data capture industry commented that screen scraping is used widely in the financial services sector as a means for retrieving consumer data and facilitates competition in the provision of consumer credit.

As part of the review, we clarified that the Code neither expressly prohibits nor endorses the use of screen scraping and that consumers are not prevented by the Code from using the services, but would do so at their own risk: see Report 718 *Response to submissions on CP 341 Review of the ePayments Code: Further consultation* ([REP 718](#)).

While at the time ASIC took this position and recognised that the operational aspects of the CDR framework would continue to evolve, ASIC does not consider that it is appropriate over the longer term for consumers to continue to use screen scraping services that are not subject to minimum protective standards when Government has introduced the CDR.

Scams, cyber security and operational resilience

Combatting scams is one of ASIC's core strategic projects.

In April this year, ASIC released Report 761 *Scam prevention, detection and response by the four major banks* ([REP 761](#)). The report identified that, between 1 July 2021 and 30 June 2022, more than 31,700 customers of the major banks lost more than \$558 million to scams. This was an increase of 49% in customers and 50% in financial losses compared to the previous 12-month period. The report also identified that bank customers were overwhelmingly the bearer of scam losses, accounting for 96% of total scam losses across the banks.

We agree that asking consumers to engage in any practice that may involve disclosure of banking login and password information to third parties runs counter to IT security practices and general guidance provided to consumers on how to avoid scams.

We also agree that screen scraping potentially increases consumers' vulnerability to scams or other malicious activity, such as phishing attacks, by increasing the number of parties who hold their login details.

Cyber and operational resilience – another of ASIC's core strategic priorities – is a critical issue for all participants in the financial system, including for entities and third-party service providers they engage with. Operationally, in ASIC's experience, screen scraping technology

can impact and slow systems and ASIC does not permit the use of screen scraping of our registry systems.

From a security perspective, recent high-profile cyber incidents and subsequent data theft from various entities demonstrate the need for all businesses to have robust cyber capabilities. Cyber-attacks are becoming more frequent and more complex. The interconnectedness of Australia's financial system means that the impact of a cyber-attack can spread well beyond a single entity. We agree with the observation in the Discussion Paper that 'despite no reported large-scale cyber security breaches of screen scraping providers to date', a data breach involving the loss of consumer banking details or passwords would likely have significant negative consequences for consumers.

We are in an environment of heightened scams and cyber risks, where Australian consumers reported losing \$3.1 billion to scams in 2022. We note that the Government is taking steps to combat scams (such as the recent launch of the National Anti-Scams Centre) and uplift national cyber security and resilience. In this setting, ASIC considers the privacy and security safeguards built into CDR make it a preferable framework for consumers to share their data rather than through screen scraping (which, as recognised in the Discussion Paper, is largely unregulated).

Consumer harms associated with screen scraping

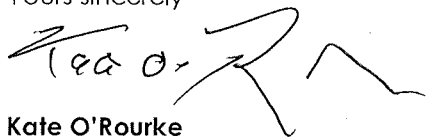
It has also come to ASIC's attention, in a matter we are currently investigating, that a credit provider has been using screen scraping for debt recovery purposes. Specifically, if a consumer is behind on repayments, the credit provider monitors their bank account to deduct funds when they become available. This has resulted in some consumers being left financially stranded and unable to meet their basic living expenses.

We note that in relation to this matter, some consumers have been unaware that their bank accounts were being accessed by a third party on an ongoing basis, despite providing initial consent.

This matter involves, in part, an example of 'write access', as referenced at page 5 of the Discussion Paper and illustrates the heightened risk of consumer harms where a third party has ongoing access to a consumer's bank account.

Please contact ASIC should you wish to discuss this feedback further.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Kate O'Rourke', with a stylized flourish at the end.

Kate O'Rourke
Commissioner

