Screen Scraping – SUBMISSION

Policy and Regulatory Implications

Jamie Leach – October 2023

FDATA A&NZ www.fdata.global

Contents

Foreword

Open Banking, a precursor to the Consumer Data Right, began as a grassroots movement, campaigning for the legal rights of consumers and businesses to have control of their financial data and share this Data with companies of their choice digitally. Given the topic of this submission, that is yet to have been achieved in Australia.

The requirement to re-examine the existing rules and to continue to finesse the technical/data standards in coordination with the initial adoption of the Consumer Data Right should be commended. Whilst the approach has varied from region to region, the principle of delivering logical, safe and understandable solutions has prevailed worldwide:

FDATA commends the Treasury Department and the Data Standards Body on their decision to review and reconsider Screen Scraping practices' role in Australia and their effects on the Consumer Data Right; however, we need to ask:

Is Screen Scraping a manifest public policy problem that necessitates Government Intervention?

We have chosen to provide a series of responses and recommendations to the topic considering the following:

- **FDATA Member's Views:** As a membership-based organisation, FDATA collects, collates, and shares the views and opinions of our members who are active participants within the banking, energy and fintech community.
- **Global Participants:** As a worldwide trade association, our experience and participation within the United Kingdom, European, North American, South American and Australasian markets influence our advice and feedback on the creation, introduction and evolution of the Open Banking and Consumer Data Right in Australia.
- **Industry Experience:** The regional representatives and associated staff of FDATA have worked within the banking, energy and financial sectors within their respective geographies. This experience is employed within the collective contribution and community discussions facilitated by FDATA's membership.

A Review into the Practice of Screen Scraping

There are two premises behind this discussion paper, with a clear indication of Governments' standpoint:

1. There is a viable alternative to Screen Scraping in Australia right now, and,
2. Screen Scraping is an inherently dangerous practice that places the consumer at risk of data breaches and requires regulatory intervention.

FDATA and our members reject both of these premises at this time.

We understand that considerable effort is being invested in raising consumer protections across Australia, as is right to do. And we acknowledge that this review and consultation have been scheduled for some time.

Of note, recommendation 2.1 of the Statutory Review stated that:

> *'screen scraping should be banned in the near future in sectors where the CDR is a viable alternative. Importantly, the Government should clearly signal when and how the implementation of the ban would take effect. This would provide certainty and adequate time for businesses to transition, along with stronger incentives to invest in moving to the CDR.'*

On 7 June 2023, the Government released its statement in response to the Statutory Review,[1] which stated that:

> *'the Government will consult on policy options to regulate screen scraping commencing in the banking sector, starting with the release of a discussion paper in the second half of 2023.'*

Industry vehemently supports the abolition of Screen Scraping; when the time is right. FDATA's members do not support that the time is right, yet. The market does not conclusively acknowledge that a viable alternative exists. In addition, considerable research has been conducted into the risk of participants, both consumers and the entities that engage in this practice.

[1] Treasury, Government statement in response to the Statutory Review of the CDR, 7 June 2023.

During the Select Committee on Financial Technology and Regulatory Technology testimony in 2020, ASIC commissioner Sean Hughes stated there is "no evidence of which [ASIC is] aware of any consumer loss from screen scraping".

Taking a similar stance, Bruce Franklin added, "I guess we're in a difficult situation that it's not a great solution, but it might be the best available."

ASIC and ACCC were reported to indicate they both have no issues with the practice, which sees third-party programs copying and collecting screen display data from another application for its own use.

Screen scraping is often described as insecure; however, in both our research and the research done by ASIC during their last review of the ePayments code, it was noted that there's never been a data breach attributable to mishandling bank credentials by a screen scraping provider — not just in Australia, but worldwide.

So, is now the right time? Is it the best solution that is available right now?

We will break our response into two sections.

1. Is there a comparative viable product available?
2. Is this practice inherently risky to consumers?

Is there a Comparative Viable Product Available?

To answer this question, we must consider what role Screen Scraping plays in the market for activities that CDR cannot yet support.

When polled, overwhelmingly, our members responded with;

Official eStatements – Most banks and non-bank lenders still require these statements to verify account ownership. Lenders also request them to support responsible lending obligations. ***CDR does not facilitate their collection nor support automation of their collection.***

The practice of scraping can collect information from multiple sources to provide a consumer product/service. Use cases for this type of collection may be in giving financial advice, accounting support, taxation preparation services, comparison products/services, etc. Whether it be datasets that include sectors not yet mandated under the CDR or the inclusion of Data Points not directed under the CDR, these Data Points/Data Sets are critical in the provision of such products/services. ***CDR does not currently have the breadth or depth necessary to compete with Screen Scraping.***

The complexities of sharing Data with consumer-consented third parties are severely challenged under the current CDR data-sharing models. Our members have outlined significant operating roadblocks for their networks of Financial Advisers, Accounting firms, Mortgage Brokers, Taxation Services, and more. The inability of a practice to provide access to the staff that would normally be involved in the preparation of products/services for their clients has created unnecessary complexity. Add to this the exclusion of critical players in the service industry, i.e. Asset Finance Brokers, Bookkeepers, and Professional Services firms, forcing the Industry to seek other methods to continue serving their clientele. ***The CDR does not allow firms or practices to share data internally under current rules. This forces the Industry to adopt alternate Data practices to comply with various pre-existing obligations.***

Under responsible lending requirements, our members also collect comprehensive data from other lender types, specifically Small/Medium Account Credit Contract lenders (BNPL, short-term loan providers, etc). These non-banking providers include Multinational brands such as American Express and Diners Club. Including these datasets can significantly affect the

appropriateness and serviceability of a lending product, such as a mortgage. ***The CDR does not cover these non-banking providers; thus, the critical data is unavailable via the CDR.***

Several FDATA members provide Intermediary services, such as Platform provision to the Mortgage Broking industry. Their established services include the ability for their customers to prefill in portions of application forms based on collected data or to commence the filling of fact-finders before service delivery. This offering has been developed to assist consumers, reduce the time to lodge applications and reduce the potential for data-entry errors and fraudulent activities. ***The CDR is read-access only and will need to be expanded to write-access for this to occur.***

Is this practice inherently risky to consumers?

The greatest risk in screen scraping and the CDR is not when Data is in transit but at rest. This is equally true of both types of data sharing. It does not pose a greater risk to those actively scraping today.

FDATA supports a mandatory security posture with collecting, sharing and retaining all Data. Industry best practices utilise a combination of heightened Consent Management Practices, Robust Encryption and Authentication Mechanisms. These security practices align with most fields our members operate within, such as dealings with the ATO, reporting to Federal Regulators, or requirements set under Cyber Insurance Compliance. Those not obligated under such frameworks have voluntarily adopted such practices to ensure their customer's data is always protected.

Many FDATA members have taken steps to become ISO27001 compliant, to achieve SOC2 certification, or to conduct their operations in line with these principles to receive the necessary Business/Cyber insurance. As such, they operate based on the SOC 2 compliance checklist and/or the ISO27001 triad compliance principles.

SOC2 Compliance

Here is a basic SOC 2 compliance checklist, which includes controls covering safety standards:

Access controls — logical and physical restrictions on assets to prevent access by unauthorized personnel.

Change management — a controlled process for managing changes to IT systems, and methods for preventing unauthorized changes.

System operations — controls that can monitor ongoing operations, detect and resolve any deviations from organizational procedures.

Mitigating risk — methods and activities that allow the organization to identify risks, as well as respond and mitigate them, while addressing any subsequent business.

Figure 1 https://www.checkpoint.com/cyber-hub/cyber-security/what-is-soc-2-compliance/

ISO27001 Compliance Triad

What are the three principles of information security in ISO/IEC 27001, also known as the CIA triad?

Confidentiality

→ Meaning: Only the right people can access the information held by the organization.

⚠ Risk example: Criminals get hold of your clients' login details and sell them on the Darknet.

Information integrity

→ Meaning: Data that the organization uses to pursue its business or keeps safe for others is reliably stored and not erased or damaged.

⚠ Risk example: A staff member accidentally deletes a row in a file during processing.

Availability of data:

→ Meaning: The organization and its clients can access the information whenever it is necessary so that business purposes and customer expectations are satisfied.

⚠ Risk example: Your enterprise database goes offline because of server problems and insufficient backup.

An information security management system that meets the requirements of ISO/IEC 27001 preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

Figure 2 https://www.iso.org/standard/27001

Common methods of adherence include, but are not exhaustive:

- The use of complex Authentication Mechanisms (Two-factor/Multi-Factor Authentication) upon staff and customers' log-in.
- The deployment of up-to-date encryption principles, both in transit and in rest.
- Data minimisation principles as required through legislative and regulatory requirements (Responsible Lending, seven-year Statute of Data Retention, etc).
- Clearly articulated, easily accessible and fit-for-purpose consent frameworks.
- Staff and operator security vetting and audits.
- Vulnerability and Penetration Testing of environments and platforms.
- Application of security protocols such as security patches, virus protection, and API monitoring.
- Limit access to job-specific need-to-know personnel.
- Third-party security sweep technology to alert of potential breach attempts and activity.
- Conformance to heightened Cloud Security protocols and deploying the full suite of environment tools (AWS, MFST, Google).

The Australian Screen Scraping community takes customer data responsibility seriously, investing time and money into the currency and suitability of their data protection practices and equipment. This is why Australia, and Globally, has not suffered a notable data breach to date attributed to the practice of scraping.

Under responsible lending regulatory guides RG209 and RG273, service operators must collect ALL required data points to support an application or provide services such as advisory/taxation preparations. Still, they are bound to verify that this information is accurate.

The narrowed scope of available data within the CDR framework restricts the ability for both data collection and verification of data accuracy to an untenable level. This abolition of scraping will force manual collection via paper documents, or worse, the act of attaching unencrypted files to an email. These antiquated practices increase the time to provision of products/services and the inherent risk to the consumer.

By restricting the ability for Screen Scraping of necessary datasets/Data Points, the risk of harm to consumers will escalate significantly. Responsible lending exists to protect consumers/customers from unnecessary, predatory and inappropriate facilities. Screen Scraping reduces the risk of unsuitable lending through the clarity and transparency of the

data. The provision of ALL necessary data, the verification of identity and the suitability of offering selected by the consumer are only possible currently through Screen Scraping. CDR is anticipated to provide this capability in the future, but it does not now.

Recommendations

FDATA supports the government's vision of providing a 'safe' manner in which data sharing can be realised in Australia. Our members believe that banning Screen Scraping without a viable alternative would negatively impact service provision in Australia and significantly disadvantage consumers and businesses alike. No one is suggesting that Screen Scraping is a long-term option. Still, there is currently NO viable alternative in Australia, and the perceived risk to consumers is not supported by evidence. Screen Scraping should be considered a transitional practice to enable uninterrupted data access until an API-based alternative can be established.

To consider banning Screen Scraping, the following would need to occur:

- The breadth and depth of CDR-mandated Data Sets would need to be expanded to cover the current data needs of consumers and businesses. Service provision of lending applications, bookkeeping services, taxation preparation, broking and similar all require access to broad Datasets/Data Points far over current CDR provisions from both a sectoral and a complexity perspective. CDR is just not enough yet.
- The CDR Models need to be amended to reflect current industry practices. Data is often shared with firms and offices, not specifically individuals. Data is touched by administration assistants, paralegals, support staff and specialists, none of which can occur under the CDR currently. This is forcing organisations to make a conscious decision about adopting the CDR.
- There is a very real need for Official Bank Statements to be shared under current responsible lending regulations and within internal lending policies. This can not occur under the CDR. A secure alternative must be sought.
- Additional sectors must be introduced to provide that viable alternative. Screen scraping is not unique to the banking/financial services sector.
- The introduction of write-access must be supercharged to enable a CDR-powered fit-for-purpose service alternative to consumers. Service provision has existed long before CDR, and if the quality of the product/service they offer is to be supported, their activities can not be restricted by unnecessary additional regulation.
- Investigations should be made into the inclusion of Personal Data Capture (Me2B wallets) that are gathering pace across the Globe and will allow the consumer/business

to share their data directly with a product/service provider. Their adoption is gaining pace across multiple sectors, from Financial Services, Health, Utilities, Travel and Government Services in some regions. We caution the Regulators and Treasury from considering that one solution will solve consumers' needs when momentum signals Consumers are choosing convenience, control and privacy, which may be through Wallets.

As per our previous responses,

FDATA supports and encourages a CDR that closely aligns with traditional practices as familiar to accredited participants but, most importantly, as familiar to the consumer. Keeping the Consumer, Choice, Convenience, and Confidence at the centre of CDR development, we commend the government and the market's continued efforts to deliver a fit-for-purpose, secure, consumer-led solution.

The ability for consumers to choose their data practices, coupled with the instant nature of digital banking, will enforce the consumers' choice to share any or all of their data for any purpose that they believe will enrich their experience or enhance their lives. In addition to suitably informed account holders, the real-time nature of data-sharing will increase the adoption of open banking and enable growth in product/service offerings for consumers and businesses alike.

The CDR is a pivotal opportunity to promote digital transformation and enhance Australia's economy, and we highly encourage the CDR to be finalised with haste to achieve these momentous objectives.

Please do not hesitate to contact me with any questions or request further input.

Kind regards,

Jamie Leach

Financial Data and Technology Association | Australia/New Zealand

Email: Jamie.leach@fdata.global | Web: fdata.global | Twitter: @FDATAglobal