Law Council
OF AUSTRALIA

Office of the President

27 October 2023

Ms Claire McKay
Acting Assistant Secretary
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

Dear Ms McKay

Discussion Paper: Screen scraping—policy and regulatory implications

1. The Law Council of Australia is pleased to make a submission to the Treasury in response to its Discussion Paper on the policy and regulatory implications of screen scraping.

2. The Law Council is grateful for the assistance of its Legal Practice Section's Australian Consumer Law Committee (**ACL Committee**) and the Queensland Law Society in preparing this submission.

Current uses of screen scraping

3. Screen scraping (also known as digital data capture) usually involves the use of technology to inspect and analyse the data contained in the browser window, either by Optical Character Recognition (**OCR**) or by converting a string of data into another format (**data parsing**) through the HTML output. This method is typically not authorised by, or necessarily within the control of, the hosting website. Whilst the website terms may seek to prohibit this practice, it can be difficult to control without extensive—and not fool-proof—back-end configuration, which is possible to circumvent.

4. The form of screen scraping that is the focus of the Discussion Paper involves consumers sharing their personal login details (i.e., for internet banking) with third parties. These third parties collect point-in-time data to provide the consumer with a service.[1] Screen scraping is used in the banking and financial services industries, as well as by energy providers and non-bank lenders.[2]

5. This specific type of screen scraping technology is widely used by banks, lenders, financial management applications, personal finance dashboards, and accounting

[1] The Treasury, Screen scraping—policy and regulatory implications (Discussion Paper, August 2023) <https://treasury.gov.au/sites/default/files/2023-08/c2023-436961-dp.pdf> 4.
[2] James Eyers, Treasury considers an end to bank account password sharing, *The Australian Financial Review* (Online, 31 August 2023) <https://www.afr.com/companies/financial-services/treasury-mulling-an-end-to-screen-scraping-in-favour-of-open-banking-20230830-p5e0rs>.

Telephone +61 2 6246 3788 • *Email* mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612 • Level 1, MODE3, 24 Lonsdale Street, Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

products,[3] with consumers' "consent", to "scrape" personal financial information from consumers' bank accounts. The financial service providers then use this information to assess the suitability of consumers' applications for financial products and services.

6. Screen scraping is commonly used to capture personal financial information about consumers in financial hardship seeking to enter into fringe lending products, such as Small Amount Credit Contracts (**SACCs**) and Medium Amount Credit Contracts (**MACCs**) as well as mortgage brokers and some banks.

7. In relation to assessing the suitability of a SACC application (for up to $2,000 for a term of between 16 days and one year),[4] the lender must obtain at least 90 days of the consumer's bank statements as part of its responsible lending obligation to consider the consumer's financial situation.[5] Lenders require consumers to provide their usernames and passwords as part of the application process so that the lenders can then access this information scraped from their banking and other financial accounts.

8. The Law Council is concerned about the practice of screen scraping in such circumstances for the following key reasons:

   - SACC and MACC lenders appear to be outsourcing their responsible lending obligations to third party screen scraping services, including to make reasonable inquiries into, and take reasonable steps to verify a consumer's financial situation.[6]

   - Consumers believe that they are providing consent for one-off access, however, terms are included in the fine print of the agreements that can enable the entity to (re)access the information at any time.

   - Reliance on disclosure, especially in standard form contracts, is a deeply unsatisfactory form of consumer protection. It is well-documented that very few individuals meaningfully engage with privacy policies or terms and conditions (particularly lengthy ones). Such disclosure rarely enables freedom of choice, particularly where consumers experiencing hardship are required to consent to screen scraping for access to products such as SACCs and MACCs.

Application Programming Interfaces

9. When considering regulatory responses, it is important to distinguish between screen scraping and Application Programming Interface (**API**) access. API is a software intermediary that allows two applications to communicate with each other.[7] The data host can monitor usage and set limits, such as authentication.

10. There are legitimate purposes to which API data can be put,[8] noting that API users typically enter into a use agreement to access the API. The use of API frameworks, such as Open Authorisation, to interface with banking and finance applications is potentially more secure than screen scraping. This is because API does not expose the

[3] Senate Select Committee on Financial Technology and Regulatory Technology (Interim Report, September 2020) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech/Interim_Report> 143.
[4] *National Consumer Credit Protection Act 2009* (Cth) s 5.
[5] Ibid ss 117(1A), 130(1A).
[6] Ibid Chapter 3 (Responsible lending conduct).
[7] Senate Select Committee on Financial Technology and Regulatory Technology (Interim Report, September 2020) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech/Interim_Report> 20.
[8] New South Wales Government, Making Data Available for Sharing (Web Page, June 2020) <https://data.nsw.gov.au/making-data-available-sharing>.

consumer's username or password, and it allows the host application (i.e., bank) and/or the user to revoke, or limit, the third party's access when no longer required.

Risks of screen scraping

11. The Law Council agrees with the risks outlined in the Discussion Paper. In addition, the **Interim Report** of the Senate Select Committee on Financial Technology and Regulatory Technology, published in September 2020, canvasses a range of risks (and benefits) associated with screen scraping use.[9] The Law Council does not seek to recite here the risks identified by the Select Committee, and trusts that the Treasury will have regard to the Interim Report in this respect.

12. Nonetheless, the Law Council emphasises the seriousness of the cybersecurity and data risks associated with providing personal login credentials to a third party, especially if those credentials are retained by the third-party recipient. Notably, the practice of screen scraping directly contradicts ongoing messaging to consumers by the Government and regulators on good online security practices, including on not sharing passwords.[10]

Consent

13. The Law Council acknowledges that the practice of screen scraping can potentially harm vulnerable consumers. If a consumer does not consent to the finance company screen scraping their data, then the application approval requirements can be very difficult for a consumer to satisfy. Screen scraping therefore has a disproportionate impact on vulnerable consumers who are required to rely on fringe lenders and to consent to screen scraping as part of their loan applications.

14. Even where a consumer's consent is given:

- such consent might not be fully informed, as the consumer might not be aware of, or able to comprehend, the technology being used and the associated risks; or

- the consent might not be freely and voluntarily given by the consumer without external influence or pressure, such as where giving the consent is included in a standard form contract, or where the consumer is under financial pressure to obtain funding.

15. As put by Jevglevskaja and Buckley:

> *… when consumers are excluded from accessing mainstream credit lines and the only available providers use SS [screen scraping], no true choice exists for consumers between obtaining credit and keeping their credentials safe. Such a scenario doesn't demonstrate conscious consumer 'demand' or choice.*[11]

[9] Senate Select Committee on Financial Technology and Regulatory Technology (Interim Report, September 2020) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech/Interim_Report> 144-150.
[10] See, eg.. Moneysmart, Protect yourself from scams (Web Page, 2023) <https://moneysmart.gov.au/online-safety/protect-yourself-from-scams>; Australian Digital Health Agency, Supporting a positive security culture: Passwords (Fact Sheet, 2020) <https://www.digitalhealth.gov.au/sites/default/files/2020-11/Passwords-Supporting_a_positive_security_culture.pdf>.
[11] Natalia Jevglevskaja and Ross Buckley, Screen Scaping of Bank Customer Data; A Lamentable Practice, *UNSW Law Research Paper No. 23-3* (9 March 2023, revised 10 July 2023) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4382528> 29.

16. There is a further risk that the consent provided by the consumer, and any data or access subsequently obtained, could be misused by the finance company, or by a malicious third party for the purpose of fraud or identity theft.

Fraud and the loss of consumer protections

17. Sharing banking passwords via screen scraping increases disclosure risks in the event of a data breach. For instance, the Commonwealth Bank of Australia has found that customers who have used the services of FinTechs relying on screen scraping are at least twice as likely to experience digital fraud, compared to those who do not share their account credentials.[12]

18. This practice also leads to the loss of consumer protections, including under the ePayments Code, which was amended in 2022 to remove the possibility of redress for victims of scams—something that consumers may not be aware of.[13]

19. The practice of screen scraping exposes consumers to potential liability for fraud, because the consumer may be in breach of their financial institution's contract terms by providing their login details to a third party. Pursuant to subclause 11.2 of the ePayments Code, if the service provider can prove, on the balance of probabilities, that a user contributed to a loss through:

    - fraud; or
    - breaching the passcode security requirements in clause 12 of the Code;

    then the consumer is liable in full for any losses that occur, until the point that this is reported to the service provider.[14]

20. While outside the scope of the Discussion Paper, the Law Council is also concerned about the use of other forms of screen scraping that do not involve consumers sharing their account login details. For example, the Law Council has received reports from its membership that the details of intellectual property right holders and applicants, published by IP Australia,[15] is scraped and used for the sending of unsolicited and fraudulent 'invoices', marketing material and scams. Similar issues are occurring with ASIC's registers of company and business names.[16]

[12] James Eyers, CBA says using fintechs exposes customers to account fraud, *Australian Financial Review* (Online, 16 March 2020) <https://www.afr.com/companies/financial-services/cba-says-using-fintechs-exposes-customers-to-account-fraud-20200316-p54amd>.
[13] David Braue, Updated ePayments Code addresses digital payments*, InformationAge* (Online, 14 June 2022) <https://ia.acs.org.au/article/2022/updated-epayments-code-addresses-digital-payments.html>.
[14] Australian Securities & Investments Commission, ePayments Code (2 June 222) <https://download.asic.gov.au/media/lloeicwb/epayments-code-published-02-june-2022.pdf> cl 11.2.
[15] See IP Australia, How to search existing designs (Web Page, 2023) <https://www.ipaustralia.gov.au/design-rights/how-to-search-existing-designs>.
[16] ASIC, Search ASIC's Registers (Web Page, 2023) <https://asic.gov.au/online-services/search-asic-s-registers/>.

Consumer Data Right

21. As noted in the Discussion Paper, the 2022 Statutory Review of the Consumer Data Right (**CDR**) recommended that screen scraping be banned in the near future in sectors where the CDR is a viable alternative.[17]

22. The CDR provides a safer and regulated means for the sharing of consumer data, including the right for consumers to withdraw consent at any time. Should the practice of screen scraping continue, the Law Council is concerned that businesses will continue to use it, instead of the CDR, despite the clear potential for consumer harm. This is because of a perception that the CDR is less convenient and efficient, and more costly and complex, than screen scraping. This is despite research demonstrating that it is unlikely that many Australian consumers would choose screen scraping, were they also given the option of sharing their data via more secure dedicated interfaces, such as under Open Banking.[18]

Next steps

23. Best practice cyber security and privacy obligations in respect of how data is collected and used should be considered in determining appropriate screen scraping policy and regulatory responses. This is particularly important in the context of the ongoing review of the *Privacy Act 1988* (Cth), including potential changes to the small business exemption.[19]

24. The Law Council's ACL Committee recommends that screen scraping, in all its forms, be banned and consumers be advised that the CDR offers a safer alternative—particularly consumers experiencing vulnerability—to control the sharing of their data. Should the Government decide to ban screen scraping altogether, a transition period that is as short as possible will incentivise the financial services sector to actively engage with the CDR (as either data holders or accredited parties), and thereby have the additional benefit of improving its functioning.

25. As outlined above, one unresolved problem with automated data sharing of this kind is that consumer consent, which is already largely fictitious—given the volume and complexity of 'click-through' agreements consumers face—is not likely to be informed. The nature, purpose and duration of access should be expressly stated in plain language before the data is shared. This should not be dependent upon a consumer opening a 'terms and conditions' link. The consent should not be able to be actioned until the use statement is provided. Even so, the reliance on any form of disclosure for consumer protection is problematic.

26. The legal profession and law practices should also understand how these technologies are used by their clients and firms, as well as their legal and ethical obligations in this regard. Due to the potential for unintended consequences, the Law Council supports its member bodies strongly discouraging solicitors from suggesting that clients share financial log-in details for the purpose of obtaining transaction data. Whilst these systems may be efficient, it is unlikely that a client will have sufficient understanding of the possible risks.

---

[17] Elizabeth Kelly PSM, Statutory Review of the Consumer Data Right (Report, September 2022) <https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf> [Recommendation 2.1].
[18] Natalia Jevglevskaja and Ross Buckley, Screen Scaping of Bank Customer Data; A Lamentable Practice, *UNSW Law Research Paper No. 23-3* (9 March 2023, revised 10 July 2023) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4382528>.
[19] See Government Response to the Privacy Act Review Report (September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.

27. Given the potentially adverse impacts on consumers, the Law Council supports, at a minimum, enhanced regulation to ensure that consumers are better protected from reliance on screen scaping services and the associated risks. Should the Government seek to proceed with the regulation of screen scraping, the Law Council would welcome the opportunity to consult further with its Constituent Bodies and Advisory Committees regarding any policy options being considered by the Treasury.

Contact

28. If the Law Council can be of any further assistance to the Treasury in the course of this consultation, please contact Mr John Farrell, Executive Policy Lawyer, on (02) 6246 3714 or at john.farrell@lawcouncil.au.

Yours sincerely

Greg McIntyre SC
President-elect