11 December 2023

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

Screen scraping – policy and regulatory implications Discussion paper

Thank you for the opportunity to contribute to the Screen scraping – policy and regulatory implications Discussion paper consultation. This submission is on behalf of the Financial Rights Legal Centre (**Financial Rights**) and the Consumer Action law Centre (**Consumer Action**).

Financial Rights is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters.

Consumer Action Law Centre is an independent, not-for profit consumer organisation based in Melbourne. We work to advance fairness in consumer markets, particularly for disadvantaged and vulnerable consumers, through financial counselling, legal advice and representation, and policy work and campaigns. Delivering assistance services to Victorian consumers, we have a national reach through our deep expertise in consumer law and policy and direct knowledge of the consumer experience of modern markets

Our organisations have consistently called for the banning of screen scraping for over a decade. Screen scraping may have been embedded in business models around the country for responsible lending checks, loan and hardship applications and other purposes, but it has done so in a regulatory gap that has enabled this dangerous and unsafe practice to flourish.

Consumer losses arising out of scams and poor data handling practices and breaches are at record levels year on year[1], harming the most vulnerable consumers in Australia. With this Australians are growing ever more aware and wary of poor data collection and handling practices.

Screen scraping is one of, if not the worst data collection and handling practices being conducted by financial services firms.

Screen scraping:

- runs directly counter to commonsense online security practices promoted and supported by government and regulators.
- disproportionately impacts on vulnerable consumers.
- increases the "attack surface" for scammers and fraudsters to infiltrate and take advantage.
- leads to the loss of consumer protections under the ePayments Code
- is a breach of bank's electronic banking terms and conditions.
- opens consumers to misconduct by a financial firm
- is unreliable and prone to errors
- acts as a barrier to financial hardship assistance
- undermines the potential success of the Consumer Data Right by allowing businesses to make cost benefit analyses in their own interest to not become CDR accredited - against the safety and security interests of their customers.

Screen scraping is an old, unsafe and dangerous technology that is fundamentally unfit for a modern, secure and safe data rich economy.

Screen scraping needs to be banned with a hard date set and as short a transition period as possible. With a program of work currently being undertaken to resolve issues in the CDR to be conducted by the end of 2024, this would be a more than reasonable date for the transition to end.

This uplift should also resolve outstanding issues in the CDR raised by consumer groups that work to undermine the safety and security of the CDR in its current form. This includes:

- reconsidering the decision to allow CDR data to be transferred to so called "trusted advisers";
- revisiting the joint account consent process which contradicts consent and safety principles;
- providing consumers with access to their own CDR data for free;

[1] ACCC, ACCC calls for united front as scammers steal over $3bn from Australians, 17 April 2023

- introducing sector specific consumer protections in line with existing regulations in each sector it is applied;
- introducing success metrics focussed on genuine consumer benefit;
- ensure that the introduction of Payment Action Initiation is safe and secure and does not increase the potential for consumer harm arising from scams;
- providing financial counsellors, community legal centres, legal aid commissions and other independent, not for profit organisation with financial support to work with the CDR and develop tools that will assist consumers; and
- ensuring that current consent review prioritises consumer interests over business interests.

No metrics or milestones should be set for the CDR to reach before a ban is implemented. Without a hard end date there will continue to be no incentive for the financial services sector to actively engage with the CDR, improve its functioning and introduce tailored solutions. Given the sector's self interest in maintaining screen scraping as the cheaper, yet unsafe alternative, any milestone set will simply incentivise the sector *not* to engage with the CDR in order to maintain its ability to rely upon the cheaper form of data aggregation.

The Australian Government has committed over $300 million to the CDR reform (including over $80 million in the 2023/24 Budget). It has done so to deliver safe, secure and easy consumer control over their data. If the CDR is ever going to work and meet these objectives in the face of industry inertia, the Government needs to make a true commitment to this reform and set a hard date to ban screen scraping.

1. What screen scraping practices are you aware of or involved in?

a. What is the scope and purpose of the data that is captured? Is the data that is captured only banking data, or does it include data from other sectors?

Financial Rights and Consumer Action work with people experiencing financial hardship on the National Debt Helpline. This work has our financial counsellors regularly requesting and examining responsible lending assessments by lenders to examine whether that lender has met their responsible lending obligations under the law. These assessments and analyses are generally obtained and conducted via a screen scraping service provided by the likes of Ilion or Proviso. We also see examples of:

- debt management firms including budgeting services using screen scraping to identify the income and expenses of their clients;
- lenders requiring screen scraping of financial information when applying for a variation on the grounds of hardship;
- mortgage brokers using screen scraping to develop loan applications and undertake analyses of loan options;
- unregulated financial services such as wage advance companies using screen scraping technology before their lending practices, and
- the not for profit Way Forward Debt Solutions (**Way Forward**) using screen scraping in in hardship applications.

Case study 1 – Way Forward[2]

Way Forward is a small not-for-profit-organisation established to explore options for getting out of debt that don't include Bankruptcy or Part IX Debt Agreements. Way Forward was created in 2018, by the four major Australian banks – Westpac, NAB, ANZ and CommBank – along with the Australian Bankers Association and the consumer movement through Financial Counselling Australia. The service is free and works with clients' creditors to establish affordable repayment arrangements.

Screen scraping has been used by Way Forward in the past to undertake analyses of client transaction data to identify debts, expenses and income to support financial hardship applications. Way Forward now conducts this information gathering and analysis exercise via a Consumer Data Right based tool.

[2] In the interests of full disclosure, Financial Rights CEO Karen Cox is a Consumer Director on the Board of Way Forward, and Way Forward CEO David Berry is the Chair of Consumer Action Law Centre

While it may be possible, we are unaware of any financial counselling agency utilising screen scraping technologies for the development of statements of financial position – a critically important and sometimes complex element of their job. We have always undertaken this work in a manual way, by obtaining statements directly from the client or their financial institution (with express client consent).

We are also aware of the use of screen scraping technologies in areas of the economy outside of the financial services sector, including:

- internet auctions,
- search engines (Google, Bing, Yandex, etc), airline, vehicle and/or holiday housing price
- aggregation,
- targeted advertising,
- website preservation,
- academic research, and
- journalism.[3]

[3] Jevglevskaja, Natalia and Buckley, Ross P., Screen Scraping of Bank Customer Data: A Lamentable Practice (March 1, 2023). UNSW Law Research Paper No. 23-3, http://dx.doi.org/10.2139/ssrn.4382528

b. What steps do consumers, screen scraping service providers and businesses using screen scraping take in the screen scraping process? What information is provided to consumers through the process?

c. When is the consumer's data accessed as a one-off, and when is longer-term or ongoing access obtained? Where ongoing access is in place, how are consumers made aware of this and can they cancel access at a later point?

We understand that many businesses who obtain passwords and usernames to screen scrape financial data do so on a once-only basis in order to obtain a point in time snapshot of transaction information to undertake analysis of income, expenses, debts and liabilities. We understand too that other services such as providers of financial management tools require and obtain ongoing access to transaction data – much of the time to ensure that the service works as promised.

However we are also aware of some lenders inappropriately holding on to passwords or log-in details, and using them at ad-hoc times for various purposes, well past the need to undertake a responsible lending check.

Case study 2 – Shelly's story - C241941

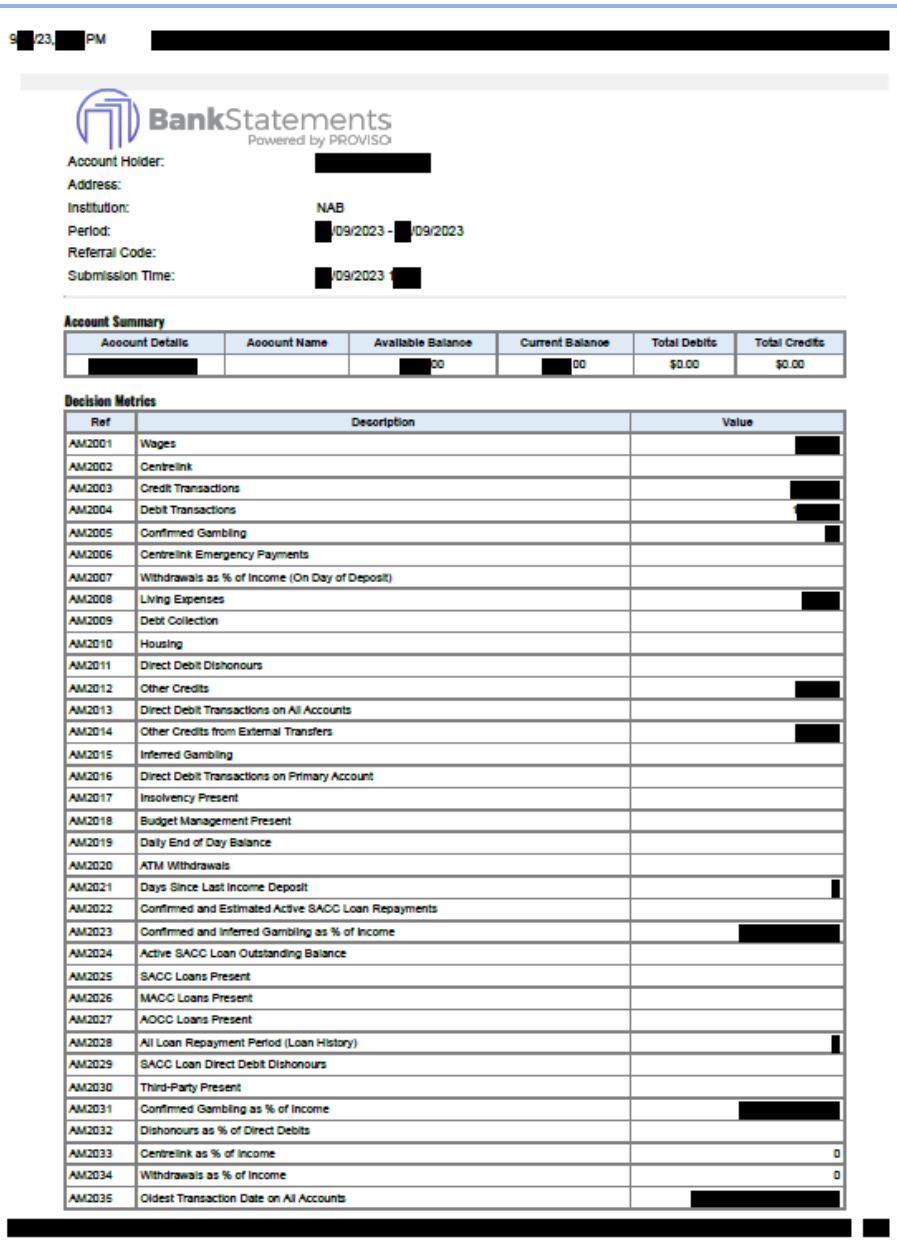
Shelly is a 20-year old Aboriginal woman diagnosed with several mental health conditions who is currently experiencing homelessness. Shelly left her family domestic violence situation when she was abruptly made homeless by her father shortly after losing her job. Whilst living in the family home Shelly was subject to physical abuse by her father.

Due to Shelly's mental health diagnosis she was able to access the Centrelink Disability Support Pension for income support. However due to affordability Shelly has been unable to find permanent accommodation and has been experiencing homelessness for the past 6-7 months.

Shelly took out a pay day loan in December 2020.

Shelly approached Financial Rights for assistance when she couldn't afford the repayments. We assisted Shelley to obtain the relevant loan documents from the fringe pay day lender. In so doing the lender provided a copy of a screen scraped bank statement current to the day we requested it. In other words, the lender was able to undertake a screen scraping exercise of Shelly's bank account over 9 months after Shelly's initial loan and at least 2 and half years after Shelly had ceased contact with the lender.

Shelley was not aware that she had provided the lender and servicescreen scraping service ongoing access to her bank account.



BankStatements
Powered by PROVISO

Account Holder:
Address:
Institution: NAB
Period: /09/2023 - /09/2023
Referral Code:
Submission Time: /09/2023

Account Summary

Account Details	Account Name	Available Balance	Current Balance	Total Debits	Total Credits
		00	00	$0.00	$0.00

Decision Metrics

Ref	Description	Value
AM2001	Wages	
AM2002	Centrelink	
AM2003	Credit Transactions	
AM2004	Debit Transactions	
AM2005	Confirmed Gambling	
AM2006	Centrelink Emergency Payments	
AM2007	Withdrawals as % of Income (On Day of Deposit)	
AM2008	Living Expenses	
AM2009	Debt Collection	
AM2010	Housing	
AM2011	Direct Debit Dishonours	
AM2012	Other Credits	
AM2013	Direct Debit Transactions on All Accounts	
AM2014	Other Credits from External Transfers	
AM2015	Inferred Gambling	
AM2016	Direct Debit Transactions on Primary Account	
AM2017	Insolvency Present	
AM2018	Budget Management Present	
AM2019	Daily End of Day Balance	
AM2020	ATM Withdrawals	
AM2021	Days Since Last Income Deposit	
AM2022	Confirmed and Estimated Active SACC Loan Repayments	
AM2023	Confirmed and Inferred Gambling as % of Income	
AM2024	Active SACC Loan Outstanding Balance	
AM2025	SACC Loans Present	
AM2026	MACC Loans Present	
AM2027	AOCC Loans Present	
AM2028	All Loan Repayment Period (Loan History)	
AM2029	SACC Loan Direct Debit Dishonours	
AM2030	Third-Party Present	
AM2031	Confirmed Gambling as % of Income	
AM2032	Dishonours as % of Direct Debits	
AM2033	Centrelink as % of Income	0
AM2034	Withdrawals as % of Income	0
AM2035	Oldest Transaction Date on All Accounts	

Source: Financial Rights Legal Centre

It is not clear to us whether there is any consistent practice in the sector as to when data is accessed in a one-off manner or in ways that are ongoing and/or ad-hoc.

We have also seen standard from credit contracts from at least one major third tier lender that explicitly clarifies that it "may access your bank account transaction information at any time during the term of your loan", as well as specifically if the borrower is in default. We consider this to be an example of an unfair contract term and does suggest that screen scraping may be used in collection activities as well.

Shelley, in **Case Study 2** was unaware that the lender had ongoing access to her bank account. Neither Jenny, nor her ex-partner in **Case Study 3** (see below) were aware that her lender had access to her ex-partner's account transaction history.

Our experience is that information regarding the risks of sharing passwords are rarely shared with consumers and if they are, they are they pointed in the direction of privacy policys which are complex and often left unread.

We are aware of at least three further examples of privacy policies that reference the specific issue of screen scraping and password use.

Pay day lender Money Me includes the following terms in their contract:

> *11.2 We may access your bank account transaction information at any time during the term of your loan. When we access your bank account transaction information, we will access your bank account transaction information going back for a period of at least 90 days from the date of access ("Transaction History") using the services of Proviso Data Pty Limited trading as Proviso Data ("Proviso")….*
>
> *11.7 Allowing us to review your Transaction History is at your sole risk* [4]

---

[4] For completeness this is the set of contractual rights that Money Me assert in accessing bank accounts

Access to your bank accounts

If you agreed to provide us with viewing access to one or more of your bank accounts, thefollowing clauses apply.

11.1 You confirm that you have provided true, accurate, current and complete information about yourself and your bank accounts (with us or third parties) and you have not misrepresentedyour identity or your account information.

11.2 We may access your bank account transaction information at any time during the term of your loan. When we access your bank account transaction information, we will access your bank account transaction information going back for a period of at least 90 days from the date of access ("Transaction History") using the services of Proviso Data Pty Limited trading as Proviso Data ("Proviso").

11.3 We may use your Transaction History to assess your creditworthiness, whether the loan you seek is suitable for you, for ongoing account management (including verification of account information), and if you are in default.

11.4 By agreeing to provide us with viewing access to your Transaction History, you authorize Proviso and Proviso's service providers to access third party sites designated by you, on your behalf, to retrieve information requested by us, and to register to view bank statements. Proviso and Proviso's service providers may, and are instructed by you as your agent and nominated representative, to access third party internet sites, servers or documents, retrieve information, and use your information with the full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection with such activities

11.5 Your Transaction History will also be used by Proviso for credit reporting body purposes and may be taken into account when producing your individual credit score, which may be shared with other organisations as part of your credit record.

11.6 When we, Proviso or Proviso's service providers access and retrieve information and Transaction History from third party sites, this is undertaken as your agent, and not the agent on behalf of any third party (including the bank account provider). Third party account providers will be entitled to rely on this authorisation and agency granted by you. This service is not endorsed or sponsored by any third party bank account providers.

11.7 Allowing us to review your Transaction History is at your sole risk. We are only able to reviewyour Transaction History on an "as is" and "as available basis" as it is made available to us by service providers. It may not be available to us from time to time.

An alternative of this contract citing Illion rather than Proviso is available here

These terms are potentially unfair on the basis that the terms are standard, the customer cannot opt out and is requiring the customer to breach their banks terms and conditions. This results in a significant imbalance of rights, is not reasonably necessary and causes detriment.

Prospa's consent to collect personal information states:

> *Bank Statements and third party account aggregation service provider: By obtaining from you access to your internet banking, our third party service provider will access your personal information for the purpose of providing your bank account information to us. We will obtain up to the last twelve (12) months bank transactions on the date you apply for a loan, in addition to further ongoing bank transactions for the term of the loan, for the purpose of assessing any future loan application or making any future offer to you. We note that your bank's terms may prohibit you from sharing your login, so you agree to appoint our third party service provider as your agent to access your internet banking on your behalf solely for this purposes and you consent to our ongoing access to this information for the term of the loan and the purposes outlined above.*[5]

Frollo's privacy policy states:

> *To access your data we will ask you to enter your banking institution account details, including username and password into your own secure-credentials-vault that is protected with bank-level 256-bit encryption.*
>
> *Frollo does not have any access to this information and purposefully uses a secure electronic platform provided by Yodlee Inc ("Yodlee") to operate the secure-credentials-vault and periodically use the bank information to link to your bank accounts and collect your recent financial data.*
>
> *The Yodlee service provides the same service to thousands of banks and financial organisations around the world. Yodlee has been subject to rigorous security due-diligence by Frollo and is compliant with international security standards. By acknowledging this privacy statement and agreeing to our Terms and Conditions you also acknowledge the Service's use of the Yodlee platform.*
>
> *Although Frollo doesn't define or control the privacy practices of Yodlee, we do regularly review their practices, performance and ongoing compliance obligations through external audits.*

Many other privacy and data collection statements that we have read do not refer to the practice at all, despite using screen scraping services.

Either way – reliance on disclosure – especially in standard forms or standard contracts - as the key form of consumer protection is deeply flawed since very few people engage with privacy policies or terms and conditions and they do little to support genuine choice or consent.

This is particularly the case with respect to vulnerable consumers experiencing financial hardship, left with little choice but to engage with fringe lenders who rely on screen scraping. As

[5] https://www.prospa.com/consent-information

Jevglevskaja and Buckley write in the research paper: Screen Scraping of Bank Customer Data: A Lamentable Practice:

> *The argument that SS [screen scraping] exists because of 'consumer demand' and 'consumer convenience' as a hassle-free way of obtaining financial services, such as small loans, is unsustainable. Faced with a choice between manually collecting, organising and presenting the required financial data in a format preferred by the lender or letting the latter obtain and collate the data, some consumers will hand over their banking credentials, and some will not. Yet when consumers are excluded from accessing mainstream credit lines and the only available providers use SS, 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. It is unlikely that many Australian consumers would choose SS were they also given the option of sharing their data via more secure dedicated interfaces as under Open Banking. …*
>
> *The asymmetry of power and information between a financially vulnerable consumer and a payday lender with access to her financial information is considerable. Even if the lender is not exploitative or fraudulent, the customer may be ill-informed, unsuspecting, or unable to properly evaluate the loan offer. Certainly, payday lending does address the financial needs of some consumers who are able to pay off the loan on time. But this industry is not built upon these responsible, savvy consumers. It is built upon the ignorant and the vulnerable, who become over-indebted and trapped, and upon the stream of late fees and other charges their credit contracts impose upon them. Overall, the practice is deeply exploitative and harms far more Australians than it assists.*[6]

For these and most other consumers, it is rare that they will engage with disclosure information. The Review of Open Banking in Australia highlighted this issue stating:

> *It is debateable whether all customers are aware of precisely what they've done in providing their login details in this way. In some cases the way in which a request for a customer's bank login details is made means that customers may not even be aware they have given their login details to someone other than their bank.* [7]

Access versus retention

Whether a service has one-off access or ongoing access, does not impact upon the ability for a firm to retain the data obtained in this process for purposes other than the direct provision of the service, including improving product delivery and analytic models. We are aware of many services who hold on to data for inappropriately extended periods depending on the interpretation of the current privacy laws - some who retain the information for *at least* seven years in line with the retention of credit information laws under Section 20W of the *Privacy Act 1988*, and others who hold on to it more or less indefinitely. This has serious repercussions for

---

[6] Pages 29 and 31, Jevglevskaja, Natalia and Buckley, Ross P., Screen Scraping of Bank Customer Data: A Lamentable Practice (March 1, 2023). UNSW Law Research Paper No. 23-3,

[7] Pag 52, Open Banking Final Report, December 2017

safety and security and very few customers would realise that their data is being used and held in this way.

And since Australians do not have a right to erasure, screen scraping provides business with the ability to hold on and use this data for as long as possible, without explicit consent. This is opposed to the CDR where consumers have the right to deletion and must provide explicit consent for further uses.

Cancellation

Regarding the ability to cancel, we are unaware of any service that provides an easy way to cancel access at a later point – certainly not in any way that would meet the requirement under the Consumer Data Right to make withdrawal of consent as easy as the provision of consent.

2. Are there any other risks to consumers from sharing their login details through screen scraping?

3. Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?

We agree with the risks – with footnoted additional information - outlined in the discussion paper that:

- screen scraping counters good online security practices[8]
- screen scraping has a disproportionate impact on vulnerable consumers and
- sharing banking passwords via screen scraping increases disclosure risks in the event of a data breach and
- sharing banking passwords via screen scraping leads to the loss of consumer protections under the ePayments Code[9]

---

[8] Examples not listed in the discussion paper include: ASIC's Money Smart website tells people that that:

> *"Don't tell anyone your passwords - a legitimate business or company should never ask you for your password."*

The Australian Government's my.gov.au initiative also recommends that:

> *"To protect your account: don't share your myGov sign in details with anybody else"*

Furthermore FinTech security and reliability may not compare with the security and reliability of financial institutions. CBA has found that customers who have used services of FinTechs relying on screen scraping are at least twice as likely to experience digital fraud, compared to customers who do not share their account credentials. James Eyers, 'CBA Says Using Fintechs Exposes Customers to Account Fraud', The Australian Financial Review, 16 March 2020

[9] It is important to note in addition to the issues listed in the discussion paper that: (a) sharing your password breaches most bank's electronic banking the terms and conditions, e.g see pages 25-26 Commonwealth Bank, Electronic Banking Terms and Conditions, 29 September 2023 and (b) consumers are likely not to realise that that they lose protection under the ePayments Code.

Needless to say, in an environment of increased losses related to scams and increasing numbers of data breaches at financial services companies, the continued green light being provided to businesses by government to screen scrape via the lack of a ban is highly problematic.

In addition to the issues listed in the discussion paper, there are a number of additional risks that need to be considered.

Screen scraping opens consumers to misconduct by a financial firm

Not only does providing password and login details to third parties open a consumer to the risk of scams, malicious activity or phishing attacks from parties other than the financial firm who obtained the password, it opens consumers up to poor behaviour from financial firms themselves. We list the following examples:

Identifying and exploiting hardship

In the past we have been aware of financially vulnerable clients providing log-in details to payday lenders, only to have the payday lender use the log-in details later to identify when a consumer is getting low on cash and subsequently directly advertising to that consumer to obtain another loan. This unfair and exploitative behaviour can lead to a consumer obtaining further monies and exacerbating their financial hardship.

While we have no direct proof of this happening recently – **Shelly's case study** above and Money Me's contract terms demonstrates that financial firms do have ongoing access to client's banking details that would easily enable this practice to take place. The mere threat that this can occur, should give pause.

Accessing other parties financial data

We are aware of financial firms screen scraping related accounts that are not held in a customer's name. This has the potential to (a) cause errors for the responsible lending assessment and (b) open up unrelated third parties to data breaches.

Case study 3– Jenny's story - C235966

Jenny is in her 40's, has 2 young children that are in her sole care and is living in a rental property. She relies on Centrelink Jobseeker (disability assessed) and Family Tax Benefit and some child support, which only in the past few months has been paid more consistently by her ex-partner. Jenny has been diagnosed with bipolar disorder and experiences poor mental health which has more recently been exacerbated by her difficult financial situation.

Jenny applied and obtained a pay day loan to pay for essential living expenses for her family. She applied for the loan online and provided some financial information during the application process, including authority for the pay day lender to access her bank statements for the 90 days prior.

In examining the credit worthiness assessment that was undertaken, the lender and screen scraper were able to screen scrape an account that was not held in Jenny's name. The account was held in her ex-partner's name and was not a joint account. Jenny is listed as an authorised operator of the account via online banking but was not the account holder.

Source: Financial Rights Legal Centre

Misleading consumers into loans

We have seen examples of firms who have misled consumers into providing details and signing them on to loan contracts without their knowledge.

Case study 4 - Edward's story - C197644

Edward was searching for good rate deals for credit on the internet. Edward found a rate on a lender's website and he then contacted them for further information. The lender then sent him an email. Edward responded and provided information to begin a process he believed would lead to him being provided with an offer. As a part of this process Edward was required to provide his details to his bank account and to obtain his credit report in order for him obtain his "tailored interest rate."

Before he knew it Edward had been approved for a $15,000 loan with the money deposited into his account. Edward had only been shopping around and had not expected to be provided with the money - merely an offer. Edward disputed he ever agreed to the loan and disputed that he had 'consented' to the loan terms, which included higher than expected fees and interest. The lender refused to rescind the contract until they had been told that he had contacted Financial Rights. In the meantime Edward had in fact found a better deal and wanted to go with this other lender.

Source: Financial Rights Legal Centre

Using screen scraping as a reason not to provide information

Finally one pay day lender we liaised with on behalf of a client refused to hand over the details of bank data that was used in a credit assessment and verification on the basis that that data is sourced "from a third party … and they contain valuable intellectual property in relation to income and expense categorisation." In other words, the fact they used a third party screen scraping service allowed them, at least in their eyes, to avoid providing basic information.

Screen scraping is prone to errors

Screen scraping is fundamentally unstable and technology breaks down regularly.[10] Screen scraping scans the existing consumer-facing web portals of financial providers, which means that if there is a small change to a website it can create stability issues for those screen scraping tools. This can lead to significant errors in calculations.

Case study 5 - Annabel's story - C196186

Annabel obtained a loan from a payday lender for $1,500. The lender uses a data aggregator with screen scraping technology to obtain required information for responsible lending checks.

In the 90 days before this loan was obtained, Annabel had entered into 2 other Small Amount Credit Contracts (SACC's) with the payday lender and was a debtor on 6 SACC's in total. This fact was noted in the loan application. Later, Annabel borrowed a further $700.

Annabel's Centrelink benefit changed from DSP to Newstart, and Annabel was unable to afford repayments at the fortnightly rate of approximately $150.

In examining Annabel's situation, Financial Rights obtained documentation from the payday lender which was based on the use of a data aggregator's screen scraping tool.

The report was riddled with inaccuracies including:

- Incorrect calculations with respect to her net monthly income which inappropriately took into account lump sum cash advance payments she received from Centrelink and assumed they were additional regular income.
- Missing information with respect to EFTPOS payments.

Source: Financial Rights Legal Centre

Difficulties in categorisation of information scraped can lead to unreliable and misleading outcomes for lending purposes.

For example, Ilion analyses and sorts transaction data into categories including: Centrelink, Fees, Gambling, Loans, Information, Overdrawn, Rent, Telecommunications, and Wages,

[10] See Tonia Berglund, 'From Screen Scraping to Open Banking', Australian Broker, 1 July 2021; Vitor Urbano, '5 Reasons Why You Should Say NO to Screen Scraping', Nordigen; Don Cardinal and Nick Thomas, 'Data Access Technology Standards' in Linda Jeng (ed), Open Banking (Oxford University Press, 2022); Roland Mesters, 'Can We Please Stop Using Screen Scraping for Bank Connectivity?', Finextra, 14 December 2021

grouping these further into income items, responsible lending flag, liabilities, expenses, and uncategorised debits. Ilion claim that they categorise about 90% of the transactions, with approximately 10% to be uncategorised.

However in our experience we see transaction data that don't have categories assigned at all. This can include items such as fast food, streaming TV services etc. In a number of the statements that we examine the high level summaries provided can show total debits equalling total credits, i.e., no surplus and yet the categorised expenses shown in the summary, when added up, give an "expense" figure that is much more modest, likely because there are items, most of which might be classified as "living expenses" which are not being factored in. This can have substantive outcomes with respect to responsible lending outcomes.

Case study 6 - Gavin's story - C196186

Gavin has payday loans totaling $4,000. In December last year he applied for loans with a payday lender where he was declined on two applications but accepted into two other loans.

Gavin has struggled to pay the loans as he has Child Support of $400 per fortnight and rent. Gavin pays $400 a fortnight to the payday lender with fees of $80 for each loan per fortnight.

The data aggregation provided for responsible lending purposes was filled with errors – including categorizing his café payments for coffee as rent.

Source: Financial Rights Legal Centre

Case study 7 - Jane and Bernie's story

Jane and Bernie were a couple with 4 dependent children. Their income derived from Centrelink and Bernie's casual job.

In late 2016 Bernie decided to purchase a car and was referred to a broker. The broker failed to properly explain the agreement they were jointly entering (even though the car was for Bernie) and Jane did not understand the relationship between the broker and the lender.

While the finance company appears to have roughly assessed Jane and Bernie's incomes correctly, it appears to have used only a one-page account scraping document pertaining to an account in Bernie's sole name, which was submitted in the loan application, to verify expenses. The finance company does not appear to have obtained copies of bank statements for Jane and Bernie's joint accounts or Jane's sole accounts at the time, which would have shown whether the loan was unaffordable for Jane and Bernie.

They soon fell into arrears on the loan as the loan was not affordable and has caused substantial hardship.

Source: Consumer Action Law Centre[11]

Requiring screen scraping for financial hardship applications can act as a barrier to assistance

As mentioned above, we have seen examples of lenders requiring screen scraping of financial information when applying for a variation on the grounds of hardship. This builds in a barrier to providing the essential support required since it (a) could put many customers off from submitting an application given the risks and (b) opens already financially vulnerable people to greater risks of data breaches, scams and a loss of rights under the ePayments Code.

Case study 8 - Zed's story

Zed was trying to negotiate a hardship variation with Zip Money. Zip Money were aware that Zed had physical issues, an acquired brain injury and was taking medication that affected his cognitive ability. They also knew that a financial counsellor was assisting him. Despite this, Zip Money contacted Zed directly stating that in order to assess his variation they would need copies of his bank statements. Zip Money stated that to make this "easier" he could supply his banking credentials to the third party company Credit Sense. Concerned about what to do, Zed got in touch with his financial counsellor for advice.

Source: Consumer Action Law Centre[12]

[11] Submission by the Financial Rights Legal Centre and the Consumer Action Law Centre Senate Select Committee on Financial Technology and Regulatory Technology Financial Technology and Regulatory Technology, December 2019

[12] As above

4. **Could you provide any examples of actions your organisation takes to prevent or block screen scraping (if you hold the consumer's data, such as a bank), or when your company's use of screen scraping has been blocked (if you provide screen scraping services or you partner with a screen scraper to provide your services), and why?**

5. **Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?**

Our organisition does not use screen scraping however we are aware of Way Forward having used screen scraping technologies with Proviso in the past.

> **Case study 1 continued – Way Forward**
>
> Way Forward managed some of the risks associated with screen scaping by providing the option to their clients to provide financial information manually. Some clients advised Way Forward that they did not feel comfortable providing their banking credentials at the login stage since it didn't feel trustworthy to people. Way Forward's team also felt uncomfortable in asking clients to use Proviso. Once the CDR went live, Way Forward decided to make the transition to CDR, despite the cost and the hurdles.

6. **Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?**

No comment

7. **Are there any other international developments that should be considered?**

No comment

8. **What are your views on the comparability of screen scraping and the CDR?**

Again our organisition does not use screen scraping and does not have direct experience of the comparability of screen scraping and the CDR. However we believe that Way Forward's experience with using screen scraping and the CDR are instructive.

> **Case study 1 continued – Way Forward**
>
> Way Forward partnered with Basiq to replace screen scraping with a CDR-based service. For Way Forward the CDR login process has been more successful in getting clients to engage with the process. Once the client selects the banking institution they need, they receive a code from their banks. According to Way Forward, by not asking clients to provide their full banking credentials, clients are more comfortable in using the service.

The key issue with the CDR for Way Forward however is that while the collection of the transaction data is accurate, the *categorisation* of this data needs to improve to ensure the accuracy of the insights and analysis undertaken. Currently Way Forward estimate that the CDR is producing 50-60 percent correct categorisation of data for Way Forward's purposes. Way Forward are currently working with Basiq to improve the data.

a. Can you provide examples of data that is being accessed through screen scraping that cannot currently be accessed using the CDR or vice versa?

No comment

b. Are there particular restrictions related to data use and disclosure under the CDR that influence choices to continue using screen scraping, or vice versa?

No comment

c. Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?

No comment

d. Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?

While we support a hard date being set, (see below) we do acknowledge that work needs to be done to improve how the CDR works re: functionality and quality of data. We understand a program of work is currently being undertaken to resolve these issues by the end of 2024.

The following additional, specific issues also need to be addressed too for consumer groups to support CDR as a safe and secure option:

Reconsider the decision to allow CDR data to be transferred to so called "trusted advisers"

Section 56AA(a)(ii) of the *Competition and Consumer Act* requires accredited persons to be the only entities able to access data through the CDR. The Independent Statutory Review report acknowledged that the current CDR regime is in breach of this section by allowing unaccredited "trusted advisors" to access CDR data. The core concern here is that the higher levels of consumer protection for CDR data are not carried through to the handling of this data by "trusted advisors', particularly those who do not meet the threshold subjecting them to the *Privacy Act*. While "Trusted Advisers" will need to be members of professions which are regulated, Treasury's own Privacy Impact Assessment stated that "those obligations can offer less protection for CDR Consumers than the strong privacy protections imposed under the CDR regime, or under the *Privacy Act*."

Revisit the joint account consent process that contradicts consent and safety principles and will lead to harm for vulnerable consumers

The CDR rules have introduced the core concept of voluntary, express and informed consent[13] which appropriately empowers consumer to make their own decisions with respect to the sharing of their CDR data. However, Treasury introduced an "opt-out" sharing model for joint account data. Under this model, joint account holders are presumed to have provided consent and need to actively opt-out of sharing data when sharing occurs. Not only is this counter to the voluntary, express and informed consent concept embedded in the rules - it undermines safety-by-design principles,[14] and is likely lead to poor outcomes especially those consumers who may be subject to economic abuse.

Provide consumers with access to their own CDR data for free

The CDR regime has failed to meet its core objective under Section 56AA(a)(i) of the Competition and Consumer Act to provide consumers direct access to their own data. The delay in progressing the "subject access" right appears partly due to legitimate fears that "forced" and/or "diverted" subject access could be used to circumvent the CDR consumer safeguards. While we agree that there is an issue – indeed we were one of the first groups to raise this as an issue with Treasury - the indefinite deferral of the direct consumer request provisions leaves a gaping hole in the CDR scheme that works against consumer interests. The scheme now only facilitates third party access to data, for a fee, with no apparent balancing right for CDR consumers to directly access and control their own CDR data via the regime.

The CDR needs to introduce sector specific consumer protections in line with existing regulations in each sector it is applied – otherwise the CDR will likely undermine those protections

The use cases that the CDR regime enables raise significant questions regarding the interaction of the CDR regime and existing consumer protections developed in each sector. For example, the CDR allows participants to obtain and use information equivalent to credit information defined and protected under the credit reporting regime.[15] In the paused telecommunications sector application, the CDR creates a pathway for government agencies to access sensitive consumer data that it is otherwise constrained from accessing through established consumer protections under the *Telecommunications (Interception and Access) Act 1979*. The sector neutral

---

[13] Rule 4.9 of the *Competition and Consumer (Consumer Data Right) Rules 2020*

[14] For further information on designing financial services products including joint accounts with safety in mind – see: Catherine Fitzpatrick. Centre for Women's Economic Safety, Designed to Disrupt: Reimaging banking products to improve financial safety, CWES Discussion Paper 1, 2022. Relevant equivalent examples in this paper include "detect, delay and block unusual patterns" and providing "Reporting functionality to provide avenues for customer concerns or employee safety concerns to be actioned" neither of which are embedded in the CDR approach; also see ASIC No-action letter – Notifying joint account holders (family violence), July 2022 that prevents notification of credit reporting information to a joint account holder, as an example of a sensible (albeit interim) regulatory approach to ensure safety for joint account those experiencing family violence

[15] Part IIIA of the *Privacy Act*, the Credit Reporting Code and the *Credit Act*

approach currently being taken is flawed and needs to ensure that extant consumer protections are not undermined by the CDR.

Introduce success metrics focussed on consumer benefit

There has yet to be any cost-benefit analysis of the CDR implementation approach nor has have consumer-centric success metrics been established. This is concerning since the government has to date provided over $300 million to the development of the regime, the industry has spent more, and consumers (and industry) have yet to see any real benefit from the regime. Without key metrics on how CDR is delivering benefits for consumers, the reform risks becoming a data-harvesting opportunity for businesses, instead of a reform that works in the interest of consumers.

Ensure that the introduction of Payment Action Initiation is safe and secure and does not increase the potential for consumer harm arising from scams

Introducing action initiation into the CDR raises the risk of fraud or misuse of data which can expose a consumer to harm. While action initiation in the CDR will not necessarily create new scam or fraud types it does introduce new opportunities for scammers, by increasing what is known as the "attack surface" for scammers and fraudsters to infiltrate and take advantage.

We understand that the action initiation regulations will apply only to the instruction layer of the process and that the CDR expansion to action initiation does not alter how the 'action layer' operates, with existing laws and practices that govern the performance of actions are intended to continue unaffected.

However this is the problem. There are few, if any, existing laws, practices, standards or consumer protections that oblige banks to detect or prevent scam activities such as impersonation, investment of phishing attack scams likely to be perpetrated against those engaging with the CDR.

Provide financial counsellors, community legal centres, legal aid commissions and other independent, not-for-profit organisations with support to work with the CDR and develop tools that will assist consumers

Treasury has long referred to potential socially beneficial use cases to support the development of the consumer data right. This includes financial counselling services obtaining and using CDR data to support their clients working through financial hardship. However obtaining access to CDR data – even as a "trusted advisor" - will require arrangements with accredited service providers to develop solutions and ongoing administration and use – all of which involves significant upfront and ongoing costs which financial counselling organisation are not funded nor resourced for. We understand that WayForward has spent a significant some of money already to do the right thing and use the CDR, with significant ongoing costs. These costs would be significantly higher in a financial counselling context due to the larger volume of clients and greater need for granular data, but they could be contained somewhat by a sector wide approach that does not require every organisation to make a separate investment. The sector would need to be supported to make this investment collectively through the peak body, Financial Counselling Australia.

If the CDR is going to work to benefit the most financially vulnerable in our community financial counsellors, community legal centres, legal aid commissions and other independent, not for profit organisations need to be supported to engage with the reform. Otherwise, financially vulnerable people will be prey to the latest set of FinTech enabled, for profit, debt management services and pay day lenders, with the resources to get ahead of the game.

The current consent review must ensure consumer interests are prioritised over business interests

Many of the current consent review proposals[16] are flawed and need to be reconsidered with a greater focus on safety and security:

- **Bundling of consents:** The proposal to bundle consents "reasonably required" for the provision of the requested service simply reinstates a core issue faced by consumers currently – that they do not engage with the use consents and take part in a tick and flick process. It also provides the unwarranted ability for businesses to deem what is "reasonably required" in their own interests, leading to a serious imbalance of power, and undermining real choice. The original Open Banking review view on bundling remains relevant. The reviewer stated that he:

  > *"considers that the use of implied and bundled consent for the data provided through Open Banking could undermine the key elements of customer control, namely that: the consent is not informed; voluntarily given; current and specific; and that the individual has the capacity to understand and communicate their consent … use cases which are particularly sensitive, consent needs to be clear, concise and effective, as well as being functional, rather than bundled with other disclosures."*

  Any movement away from these core principles simply removes the choice and control for consumers that is at heart of the CDR. Further the consumer testing undertaken to justify the position is flawed since it did not test people's views of bundling where things went wrong. This is the value consumer representative input can provide since consumer representatives witness and deal with things when they go wrong.

- **Preselected and actively selected options:** We remain of the view that consumers be provided the ability to unclick datasets that are essential for a service to function. Unclicking the option should then provide the information that the service would not be able to work. This action may seem the same as indicating what is required – but simply providing the ability for some to engage with the process has at a minimum the potential to promote greater understanding of the use case and collection by encouraging and enabling engagement, rather than not reading the information and moving on.

- **Withdrawal of consent information:** We disagree with the proposal to remove the requirements to include instructions on how to withdraw consent in the consent flow. This is because people motivated to sign on to are service are generally more engaged during the on-boarding process than at other times, other than when things go wrong.

---

[16] Treasury, Consumer Data Right rules – Consent Review and operational enhancements design papers, August 2023

Removing it from this process and essentially hiding this information in a receipt that is likely not to be read is disempowering when disclosure and consent are the only real consumer protections in CDR. We also remain concerned with the proposal to no longer state the consequences of withdrawing a consent at the time of giving consent, and only including these consequences at the time of withdrawal. We oppose this since it means that the withdrawal of consent is now more difficult than granting it and it embeds a potential dark pattern where a business can present the consequences of withdrawal in such a way that it could become a subscription trap. This has the real potential of undermining trust and confidence in the CDR regime which is meant to be the safer and more secure than the alternative.

- **Supporting parties:** Presentation of supporting parties in the consent flow must involve providing the high level details of their names on the collapsed view. This is the principle that informs other sections of the collapsed view – the same should be applied to supporting parties. This could also prompt people to engage with the information, promoting improved disclosure and control.
- **De-identification and deletion by default:** We strongly support the proposed deletion by default approach to redundant data handling.

9. The Statutory Review recommended that screen scraping should be banned in the near future in sectors where the CDR is a viable alternative.

a. How should the Government determine if the CDR is a viable alternative?

b. What are your views on a ban on screen scraping where the CDR is a viable alternative?

Set a hard date to ban screen scraping with as short a transition period as possible

Screen scraping needs to be banned with a hard date set now and as short a transition period as possible.

Any decision to allow screen scraping to continue unchecked simply provides government approval for dangerously unsafe and insecure data handling practices, and serves to undermine the success of the CDR reform.

Without a hard end date there will continue to be no incentive for the financial services sector to actively engage with the consumer data right (as a data holder or accredited party) and improve its functioning.

For many in the industry, the CDR is seen as too costly, too hard, or involves too much "red tape". In support of maintaining screen scraping, industry variously argues that screen scraping is convenient, efficient, low cost or even free, does not require entering into contractual arrangements with data holders, and does not require accreditation which is timely, expensive and complex. Another benefit for business models relying on screen scraping is the ability to retain consumer data (de-identified or otherwise) for extended periods without explicit

consent, and the inability of the consumer to have their data deleted, as required under the under CDR.

These arguments have led the majority of FinTechs and financial services to make business-led cost benefit decisions to not move to CDR and continue to rely on the legal data aggregation process of screen scraping. In doing so they have chosen their own bottom-line interests over the security and safety needs and best interests of their customers.

The continued ability for financial services to legally engage with the unsafe, insecure yet cheap practice of screen scraping legal is also *the real* reason that there has been low uptake of the safer and more secure CDR by industry and consumers. Businesses will always have an interest in holding on to outdated business models where it is cheaper for them to do so yet risky and unsafe for their customers.

Setting a hard date to end the alternative pathway afforded by screen scraping is the only way to ensure that the sector will move to the CDR, which will in turn increase resources into its iterative improvement, and lower costs for all.

We do not support the setting of particular milestones beyond which will trigger a ban of, or transition away from screen scraping. The reasons are threefold:

First, there are currently few metrics available to measure success of the CDR. There has yet to be any cost-benefit analysis of the CDR implementation approach nor has have consumer-centric success metrics been established.

Second, given the sector's self interest in maintaining screen scraping as an alternative, as outlined above, any milestone set will simply incentivise the sector *not* to engage with the CDR in order to not meet the milestone and maintain its ability to rely upon the cheaper yet unsafe form of data aggregation that works for businesses not consumers.

Finally, the Australian Government has committed over $300 million to the CDR reform (including over $80 million in the 2023/24 Budget). CDR was introduced to enable and deliver safe, secure and easy consumer control over their data. If the CDR is ever going to work and meet these objectives, the Government needs to make a true commitment to this reform and set a hard date to ban screen scraping.

c. What timeframe would be required for an industry transition away from screen scraping and why?

As expressed above, screen scraping needs to be banned with a hard date set with as short a transition period as possible.

We do note that there has been a pause placed on the development of the CDR until the end of 2024 to "allow time to focus on ensuring that the CDR in banking is working as effectively as possible, extending into the non-bank lending sector and continuing with the energy rollout as

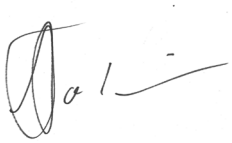
planned."[17] Given this consolidation it makes sense to set the date to line up with the end of this consolidation period.

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights Senior Policy and Advocacy Officer, Drew MacRae at drew.macrae@financialrights.org.au.

Kind Regards,

Karen Cox
Chief Executive Officer
Financial Rights Legal Centre



Stephanie Tonkin
Chief Executive Officer
Consumer Action Law Centre

[17] Consumer Data Right insurance rollout put on hold, Insurance News 5 June 2023