Submission by the

Financial Rights Legal Centre and Consumer Action Law Centre

Australian Competition and Consumer Commission

Consumer Data Right: Consultation on how best to facilitate participation of third party service providers, December 2019

February 2020

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 | info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre 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. Financial Rights took over 22,000 calls for advice or assistance during the 2018/2019 financial year.

About the Consumer Action Law Centre

Consumer Action is an independent, not-for profit consumer organisation with deep expertise in consumer and consumer credit laws, policy and direct knowledge of people's experience of modern markets. We work for a just marketplace, where people have power and business plays fair. We make life easier for people experiencing vulnerability and disadvantage in Australia, through financial counselling, legal advice, legal representation, policy work and campaigns. Based in Melbourne, our direct services assist Victorians and our advocacy supports a just market place for all Australians.

Introduction

Thank you for the opportunity to comment on the Australian Competition and Consumer Commission's Consumer Data Right: Consultation on how best to facilitate participation of third party service providers. This submission is made on behalf of the Financial Rights Legal Centre (**Financial Rights**) and the Consumer Action Law Centre (**Consumer Action**).

Our organisations have expressed concern with the potential ability for Consumer Data Right (**CDR**) data to be disclosed to, and obtained by, non-accredited third parties in multiple submissions over the development of the Consumer Data Right. In Financial Rights' submission to the Senate Inquiry into the Consumer Data Right legislation,[1] for example, we highlighted that the CDR facilitates the leaking of sensitive financial data to entities that provide lower privacy protections and that this is a fundamental flaw to the legislation and needs to be reconsidered.

We noted that the concerns of consumer representatives with respect to the potential for CDR data to leak outside of the system was at that time "somewhat ameliorated temporarily under the first iteration of the ACCC rules.[2]" We then went on to note that:

> *there is no guarantee moving into the future that this will remain the case. Indeed it is highly likely that they will at some point available to non-accredited parties in future iterations of the ACCC CDR Rules.*

Consideration to allowing the leakage of voluminous, highly sensitive financial data outside of the protections afforded by the CDR regime has come sooner than expected, and before real world testing of the regime has begun.

We remain of the view that no non-accredited third parties should be permitted to receive CDR data and that it is inappropriate for any unaccredited third party to receive and hold CDR data. Allowing for such an ability fundamentally undermines the entire point of the Consumer Data Right regime in promoting safer and more secure data practices, and will likely lead to a lack of consumer confidence in the regime as soon as the inevitable first breach occurs.

If, against the advice of consumer groups, it is decided that non-accredited third parties are permitted to receive CDR data then one of the following options must be implemented to

---

[1] Submission by the Financial Rights Legal Centre Senate Economics Legislation Committee Inquiry into Treasury Laws Amendment (Consumer Data Right) Bill 2018, February 2018 https://financialrights.org.au/wp-content/uploads/2019/03/192028_SenateCDRInquiry_Submission_final.pdf

[2] Rule 8.8, ACCC CDR Rules Outline, December 2018, "*The ACCC does not propose to include sharing of CDR data with a non-accredited entity in version one of the Rules. This is in light of concerns from stakeholders that transfer of CDR data to a non-accredited entity risks undermining the consumer protection that the accreditation process is designed to provide. The ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) will be considered for inclusion in the next version of the Rules.*"

ensure that the privacy and consumer protections of the CDR regime are extended to those consumers:

- Strengthened privacy safeguards should be extended to all consumers in all situations;
- A new accreditation tier be created;
- Warnings should be provided; and
- Screen-scraping should be banned.

Non-accredited third parties should also meet CDR Rules appropriate to their role and should have appropriate administrative and procedural protections place to protect consumers. The same consent and notification requirements that apply under the CDR rules should apply to the passing of CDR to a "non-accredited Third Party."

Finally if as conceived under the consultation paper with respect to intermediaries, tiered accreditation is introduced, it should be done so in a form that does not undermine or compromise consumer privacy, safety and security.

Our submission begins with this latter point in the order presented in the consultation paper, and then moves on to the issue of non-accredited third parties.

Intermediaries

We are not opposed to a tiered accreditation regime that takes into account the different roles of different entities within the CDR system including intermediaries.

However, in designing these tiers, consumer data safety and security must be prioritised. It is critical that no loopholes or exemptions are put in place for CDR data holders, recipients or intermediaries to take advantage of Australian consumers or undertake any form of regulatory arbitrage or avoidance.

We are concerned with the FinTech sector's approach to the CDR. Financial Rights has attended a number of Data 61 workshops on the consumer experience of the CDR. We found that many FinTechs (and intermediaries) in these workshops would openly put forward ideas for ways FinTech's could get around the rules that have been set. Some of the ideas included finding, confirming and exploiting loopholes in the rules, and developing user experiences that limit consumer ability to control their engagement with the applications and their data like dark patterns - tricks used in apps that make you buy or sign up for things that a user didn't mean to.

There have been a number of examples of this:

- One FinTech representative stated that they had figured out a loophole to the CDR regime where unaccredited FinTechs[3] can simply ask for people to hand over the data

[3] Or the clients of Fintechs using their services

that the consumers themselves request directly from their data holder. These FinTechs/companies would therefore not have to get accredited. This FinTech asserted that they planned to be exploiting this loophole from 2022.

- Another FinTech representative believed that CDR Data Recipients will be able to offer consumers something in return for consenting to the holding or de-identification of data - that is they plan to have their client FinTechs offer movie tickets, vouchers, cash or other financial incentives to consent to the collection and retention of de-identified data.[4]

This approach from the FinTech sector is unsurprising: self-interest and pursuit of profit at the expense of consumers drives regulatory arbitrage in most sectors. It nevertheless remains disappointing.

What it will require though is well resourced regulators to provide adequate oversight, amend and improve the standards, and recommend changes to the governing legislation, wherever FinTech arbitrage leads to demonstrably poor consumer outcomes. Ensuring appropriate regulatory protections are in place will enhance effective competition and innovation and give consumers confidence that their engagement with service providers is safe, secure and will not lead to consumer harm.

We therefore believe that the development of any tiered accreditation must ensure that the accreditation regime does not enable any regulatory arbitrage to take place nor undermine consumer privacy, safety and security with respect to their customer's sensitive financial data.

Recommendation

1. **Tiered accreditation should be introduced in a way that does not undermine or compromise consumer privacy, safety and security.**

[4] Further examples are detailed in the Joint Consumer Submission to the Senate Select Committee on Financial Technology and Regulatory Technology https://financialrights.org.au/wp-content/uploads/2020/02/191223_FinTechInquiry_Sub_FINAL.pdf

Permitting CDR data to be disclosed to non-accredited third parties

8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

It is our strong view that no non-accredited third parties should be permitted to receive CDR data and that it is inappropriate for any non-accredited third party to receive and hold CDR data.

The Open Banking Review Final Report recommended that the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity.

> ***Recommendation 2.7 accreditation***
>
> *Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.*[5]

The reasons for a closed system were detailed as follows:

> *Accreditation would create a list of parties who are considered trustworthy, due to their compliance with a set of requirements. A customer's banking data is valuable information and its misuse can lead to damage or financial loss. Those who receive and hold data under Open Banking should therefore be required to safeguard that information.*
>
> …
>
> *From the customer's perspective, an accreditation process is desirable. Accreditation would allow customers to determine with greater ease which data recipients meet the Standards and may, as a result, be considered trustworthy. An accreditation process should inspire confidence amongst customers to share their data with recipients that the customer has chosen to trust. An accreditation process would also provide some level of customer protection from malicious third parties.*

The Report also noted that there is a closed system within the only other major developed country with Open Banking.

> *The UK has decided to limit access only to accredited third parties known as 'whitelisted parties'. A bank would only comply with a customer's request to transfer their data to a third party if that party is 'whitelisted'. This limitation of access reduces risk and gives users greater confidence in sharing data. The EU's PSD2 also contains an accreditation process.*

All handlers of CDR data – from banks and credit unions (data holders), FinTechs and software developers (data participants) to accountants, financial advisors, mortgage brokers, insurance brokers, landlords or any other entity with even a remote interest in gaining access to sensitive, personal financial data – should be accredited.

---

[5] Open Banking: customers, choice, convenience, confidence, December 2017 https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

Accreditation for all those parties interested in using CDR can be done so on a sliding scale if need be. However critically it would ensure that consumers taking part in the CDR will be able to avail themselves of the strengthened privacy safeguards afforded under the CDR regime.

Varying levels of privacy protection

The introduction of the CDR regime has created multiple levels of privacy standards for different people that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

- CDR Privacy Safeguards– essentially strengthened versions of the Australian Privacy Principles (**APPs**);
- the *Privacy Act* safeguards as detailed under the APPs; and
- general consumer protections and law applying to those holders of consumer data that are *not* "APP entities" as defined under the APPs, ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million.

If non-accredited parties are to be able to access CDR data, this will lead to the following two situations that provide lower standards of consumer protection:

1. CDR data accessed and held by non-accredited parties who are "APP entities"[6] will be subject to the APPs, not the CDR privacy safeguards.
2. CDR data accessed and held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

Allowing non-accredited CDR participants the ability to access CDR against the recommendation of the Open Banking Report creates a significant leakage point for CDR data to fall outside of the system, whereby consumers will be provided fewer or lower standard protections or in some cases, no realistic privacy protections at all if or when a breach or problem arises out of the use or misuse of this CDR data.

The risks bear repeating.

- *Fewer, if any, security requirements increases the likelihood of a breach:* Non-accredited third parties holding CDR data are more likely to be breached, given stronger security requirements under the CDR will not apply to them;
- *Identify theft:* If breached sensitive financial data can be used for identity fraud by a bad actor;
- *Material theft:* If breached sensitive financial data can be used to access funds by a bad actor;

[6] Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses

- *Fewer consumer rights:* If anything were to go wrong, the protections and rights afforded by the CDR will not apply.

We note that the ACCC states in the consultation paper that:

> *The ACCC recognises there are existing mechanisms that facilitate the transfer of data from consumers to third parties.*

In other words – if non-accredited third parties were to be able to access CDR data – then this is really no different to what is occurring now.

It may be true that third parties are be able to access financial data currently but the entire point of the CDR – its entire reason for being - is to make the access to and transfer of high sensitive financial data safer, more secure and consistent. It is meant to improve what occurs by encouraging consumers to share their data within a safe and secure system with the confidence and assurance that their privacy will be protected. Allowing the easy, faster transfer of CDR data to non-accredited third parties without the same consumer protections as expressed under the CDR privacy standards is to fundamentally undermine the entire point of the CDR and will lead to both poor outcomes for consumers and has the very real potential to undermine the success of the CDR altogether.

Any decision to allow non-accredited third parties to access sensitive CDR data is incredibly dangerous. It is dangerous because consumers are being led to assume their data will be protected under a "Consumer Data Right" but in fact it is facilitating the movement of this data to lower privacy protections.

Solutions

The key principle the CDR regime must meet with respect to the use of CDR data is that consumers who choose to use and pass on their CDR data are afforded all the privacy and consumer protections under the CDR regime no matter who holds them – including data holders, accredited CDR participants and other third parties currently conceived under the umbrella term of non-accredited third parties.

This can be accomplished in a number of ways.

Extend strengthened Privacy safeguards to all consumers

Extending stronger privacy safeguards could be achieved by amending and strengthening the *Privacy Act* and the APPs to ensure that the same stronger protections under the CDR apply to all consumer data wherever it exists. We note that the ACCC and the Government have made some gestures towards implementing just this solution in the Government's response to the Digital Platform Inquiry including a review of the Privacy Act to

> *"…ensure it empowers consumers, protects their data and best serves the Australian economy. A review will identify any areas where consumer privacy protection can be improved, how to ensure our privacy regime operates effectively for all elements of the community and allows for innovation and growth of the digital economy*

Introduce a new accreditation tier

The CDR can and should accommodate the use cases captured in response to Question 7 of this current consultation[7] by designing an accreditation system that appropriately extends the consumer protections of the CDR to these use cases and sets accreditation standards that appropriately reflect the different role played by potential entities who are currently considered non-accredited third parties, such as accountants, real estate agents etc. This may involve reduced requirements, but should include all the safety and security requirements that would ensure consumers remain protected. This submission addresses accreditation criteria in answer to questions 8 and 9 below.

Provide warnings

While not a solution, an option that must be considered is to include a warning to consumers to state that the protections under the CDR will not apply. We note that this is in fact the Maddocks' Privacy Impact Assessment Recommendation 3.2, that is to:

> *include an obligation on Data Holders to "warn" CDR Consumers when providing them with their CDR Data pursuant to their request (for example to state that the protections of the CDR regime (and possibly the APPs) will not apply if they provide that data to a third party). Similarly, if an Accredited Data Recipient discloses CDR Data to the CDR Consumer (which is a 'permitted use' of that CDR Data), indicate whether a similar protection is required in these circumstances;*[8]

We also note that the subsequent Agency Response puts forward two arguments against taking this action. Firstly:

> *The privacy risks associated with providing human readable data directly to the consumer is lower than the risks of providing machine readable data, being similar to the risks associated with consumers currently having an ability to view their own bank statements.*[9]

Subsequently the Agency Response states:

> *The suggested "warning" may unduly discourage consumers from accessing their data through the CDR regime in a situation where privacy implications are lower than for other methods of data sharing, such as screen scraping, for which no warnings would be required.*

We adamantly reject these arguments.

---

[7] That is: "7. If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited third parties and you intend to: a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers; b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers."

[8] Page 10, Maddocks, Department of the Treasury, Consumer Data Right Regime [Analysis as at 23 September 2019], PIA report finalised on 29 November 2019

[9] Page 8, Treasury, ACCC, OAIC, Data61, Consumer Data Right Privacy Impact Assessment Agency Response, December 20 9

Firstly is not clear from this current consultation whether the disclosure of CDR data to non-accredited third parties would be done so in human readable format or machine readable format. Either way we maintain that protections for consumers must be provided.

With respect to the case where CDR data provided to non-accredited third parties would be restricted to human readable formats - all human readable material is currently machine readable anyway through scanning technology. Any Adobe PDF reader can do this right now and can be combined with screen scraping technology to extract the appropriate data. While this is more complex, it is still worth it for many entities to undertake this process.

With respect to the risk "being similar to the risks associated with consumers currently having an ability to view their own bank statements" again we point out that

a. the CDR produces higher volume, more detailed data, at greater speed; and
b. the CDR is meant to create a safer and more secure system to what currently exists.

With respect to warnings unduly discouraging consumers from accessing their data through the CDR – we reject that any warning here is undue. The risks are just as bad or worse as they are for existing forms of access, because of the higher volume, more detailed data that can be accessed at greater speed, - albeit through a slightly more complex extraction process as described above.

Even if it were to be conceded that the risks were lower, not providing a warning to consumers of the very real risks that exist would be a derogation of the duty of regulators of the CDR to keep consumer data safe at the same time as encouraging consumers to take part in the CDR. If the agencies overseeing the CDR choose not to provide a warning, then they take the real risk of fundamentally undermining consumer confidence in the CDR the first time a significant breach occurs.

We do note that warnings may not be sufficient to mitigate against the risks involved. Recent ASIC research found that:

> *There is emerging evidence from financial services regulators about the limitations of the effectiveness of warnings that firms have to display about the risks and features of certain products and services. … Warnings are not a cure-all for problems in financial services markets.*[10]

We agree with ASIC that warnings are insufficient and should not be seen to be as a solution. Nevertheless, warnings could play a minor role in preventing a small proportion people from engaging in risky behaviour.

[10] Page 5, ASIC Rep 632: Disclosure: Why it shouldn't be the default A joint report from the Australian Securities and Investments Commission (ASIC) and the Dutch Authority for the Financial Markets (AFM) https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf

Ban screen-scraping

If the delivery of CDR data to non-accredited parties is limited to human readable formats, another solution to prevent misuse of the data would to ban screen scraping – as the UK and EU have done.

We have outlined why screen-scraping must be banned alongside the introduction of the CDR regime in our recent submission to the Senate Select Committee on Financial Technology and Regulatory Technology's inquiry into Financial Technology and Regulatory Technology. We have attached the section detailing the full reasons why this is the case at **Attachment A**.

Recommendations

2. **No non-accredited third parties should be permitted to receive CDR data and that it is inappropriate for any unaccredited third party to receive and hold CDR data.**
3. **If it is decided that non-accredited third parties are permitted to receive CDR data then one of the following option must be implemented to ensure that the privacy and consumer protections of the CDR regime are extended to those consumers:**
    a. **Extend strengthened Privacy safeguards to all consumers;**
    b. **Introduce a new accreditation tier; and/or**
    c. **Provide warnings.**
4. **Screen-scraping should be banned.**

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

As we have noted we do not support the concept of an accredited person being able to transfer CDR data to a non-accredited third party.

It is essential that *all* the strengthened privacy and consumer protections afforded consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by a non-accredited third party. The same strong sanctions and remedy regime should also be applied to non-accredited third parties.

This means that the following Privacy Safeguards should apply and would substitute the APPs:

- Privacy Safeguard 1. Open and transparent management of CDR data
- Privacy Safeguard 2. Anonymity and pseudonymity
- Privacy Safeguard 6. Use or disclosure of CDR data
- Privacy Safeguard 7. Use or disclosure of CDR data for direct marketing by accredited data recipients and designated gateways

- Privacy Safeguard 8. Cross-border disclosure of CDR data
- Privacy Safeguard 9. Adoption or disclosure of government related identifiers
- Privacy Safeguard 10. Notifying of the disclosure of CDR data
- Privacy Safeguard 11. Quality of CDR data
- Privacy Safeguard 12 Security of CDR data; and
- Privacy Safeguard 13 Correction of CDR data

Non-accredited third parties should also meet the following as set out under the CDR Rules:

- Consent requirements
- Deletion and de-identification of CDR data rules
- Notification rules.

We also believe that non-accredited third parties should have the following in place:

- internal dispute resolution processes;
- be a member of a recognised external dispute resolution scheme;
- have addresses for service;
- have adequate insurance;
- establish a formal governance framework for managing information security risks relating to CDR data;
- have and maintain an information security capability
- meet minimum information security controls;
- have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.

Recommendations

5. **All strengthened privacy and consumer protections provided to consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by a non-accredited third party.**
6. **Non-accredited third parties should also meet CDR Rules appropriate to their role and should have appropriate administrative and procedural protections place to protect consumers.**

10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?

Again, as we have noted we do not support the concept of an accredited person being able to transfer CDR data to a non-accredited third party.

If this were to nevertheless occur, it is essential that at the very least a warning is provided to the consumer who intends to act in this way. To not provide a warning would be to place consumers at serious risk.

Furthermore, we believe that the same consent and notification requirements that apply under the CDR rules should apply here. The reason for this is clear. The same safety and security issues arise when a non-accredited third party receives CDR data holds data as they arise with an accredited party.

Specifically consent must be given by a CDR consumer to a recipient to collect and use CDR data and that is:

(a) voluntary; and

(b) express; and

(c) informed; and

(d) specific as to purpose; and

(e) time limited; and

(f) easily withdrawn.[11]

Recipients of CDR data should meet the consent rules under the CDR Rules including:

- asking CDR consumer to give consent to collect and use CDR data, including the information they need to present to the CDR consumer when asking for consent: Rule 4.11;
- restrictions on seeking consent should be in line with the requirements: Rule 4.12.
- rules regarding the withdrawal of consent to collect and use CDR data and notification: Rule 4.13;
- limits on the duration of consent to collect and use CDR data: Rule 4.14;
- information relating to de-identification of CDR data: Rule 4.15
- rules regarding the election to delete redundant data: rules 4.16-4.17

We also believe that the notification requirements under Subdivision 4.3.5 should apply.

As mentioned above, recipients should also meet the rules with respect to the authorisation to disclose CDR data.

[11] 4.9

Whether non-accredited third parties should have to maintain consumer dashboards etc given they are not creating apps, is unclear but may depend on use cases presented.

Recommendations

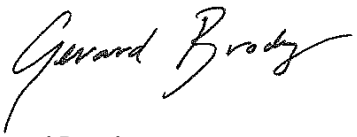
7. **The same consent and notification requirements that apply under the CDR rules should apply to the passing of CDR to a "non-accredited Third Party."**

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 Drew MacRae, Policy and Advocacy Officer, Financial Rights on [redacted].

Kind Regards,

Karen Cox
Chief Executive Officer
Financial Rights Legal Centre



Gerard Brody
Chief Executive Officer
Consumer Action Law Centre

Attachment A:

Extract from the Submission by the Financial Rights Legal Centre and the Consumer Action Law Centre, Senate Select Committee on Financial Technology and Regulatory Technology, Inquiry into Financial Technology and Regulatory Technology, December 2019

Prohibit the dangerous practice of screen scraping

For the government's Consumer Data Right to succeed and build high levels of consumer confidence and trust in a safe and secure FinTech sector, the outmoded and dangerous practice of screen scraping must be prohibited.

What is screen scraping?

Screen scraping is the process by which screen display data is obtained and translated from one application to another. It usually involves a consumer providing their log-in credentials (eg username and password) to a third party (such as a payday loan operator) who then uses these to access the data held by another party (such as a bank) via a customer-facing website. Consumer data is then collected from the website for various purposes.

Screen scraping is ostensibly used in the lending sector to undertake responsible lending checks and is prevalent throughout the small amount credit contract market. The case studies below demonstrate the flaws and risks when this technology is relied on by lenders to undertake lending checks:

Case study Annabel's story - C196186

About 2 years ago, Annabel got a loan 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.

Annabel borrowed a further $700 in 2018.

Last September, 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

Case study Jane and Bernie's story

Jane and Bernie (names changed) 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.

Both the broker's loan application and finance company's assessment appear to significantly understate Jane and Bernie's living expenses, with the expenses listed on the lending assessment document totalling even less than that on the loan application. The finance company appears to have applied an arbitrary benchmark that was lower than both the Henderson Poverty Index (HPI) and Household Expenditure Measure (HEM) benchmarks for that quarter.

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

Source: Consumer Action Law Centre

In the Australian market screen scraping technology is provided by the likes of the US-based Yodlee, Adelaide based Proviso and Sydney-based Basiq.

Screen scraping that Financial Rights see produces documents that break down incomings and outgoings in consumer accounts detailing categories such as wages, Centrelink payments, SACC loans, Groceries, Fees, Telecommunications expenditure etc.

The information provided can be useful for lenders if used responsibly and appropriately but there are a significant number of problems with the practice – many of which can be and are now resolved by the Consumer Data Right.

What is wrong with using screen-scraping technologies?

The problems with screen scraping data aggregators are numerous and include the following:

Screen scraping requires unsafe online practices actively deterred by government and industry

The basic procedural premise of screen scraping is it requires a consumer to hand over their password and username details in order to access and analyse their data. This is an inherently unsafe online practice and is exactly the opposite to every other piece of online safety and security advice provided to Australians by both the online industry and in government advisories.

For example, 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."*[12]

The Australian Government's StaySmartOnline website states:

> *"Keep your passwords secure by taking measures to protect them: Don't share your passwords with anyone."*[13]

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*[14]

It is a dangerous practice to hand over one's password details because encouraging such a practice makes passwords and security information more vulnerable to breach and can lead to people being scammed, people having their identities or money stolen or worse. It is also dangerous to hand over password material to FinTech and financial services providers.[15]

---

[12] https://www.moneysmart.gov.au/scams/avoiding-scams

[13] https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/passwords-business

[14] https://my.gov.au/mygov/content/html/security.html

[15] We note that FinTech Australia report that "between 10-50 per cent of potential customers baulk at handling over their passcode" https://treasury.gov.au/sites/default/files/2019-03/c2017-t224510_FinTech_2.pdf. This is because it is an inherently unsafe practice and consumers are well-advised not to do so.

Case study Zed's story

Zed (name changed) was trying to negotiate a hardship variation with a Buy Now Pay Later Service. The Buy Now Pay Later Service 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, the Buy Now Pay Later Service contacted Zed directly stating that in order to assess his variation they would need copies of his bank statements. The Buy Now Pay Later Service stated that to make this "easier" he could supply his banking credentials to a third party company. Concerned about what to do, Zed got in touch with his financial counsellor for advice.

Source: Consumer Action Law Centre

We are 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 advertise to that consumer. This has the effect of exacerbating financial hardship.

The Financial Services Royal Commission made explicit recommendations against the hawking of superannuation and insurance noting that "the practice has long been unlawful because it too readily allows the fraudulent or unscrupulous to prey upon the unsuspecting."[16] A ban on hawking should also capture online hawking that can result from unsafe practices such as screen scraping.

The asymmetry of power and information between the payday lenders with access to someone's financial information and that individual is immense. Even if the 'hawker' was not fraudulent or unscrupulous, the customer may be ill-informed, unsuspecting, or lacking knowledge and is not prepared to critically evaluate the offer.

Provisions set out in the *Corporations Act 2001*[17] prohibit offering financial products for issue or sale during (or because of) an unsolicited meeting or 'cold' telephone call - but these scenarios imply that the hawker is a human exercising agency.

We encourage this Committee to recommend amending both the law, and ASIC regulatory guidelines for hawking (RG 38 (2005)), to capture digital or online hawking.

Our organisations regularly hear of other dodgy practices:

[16] Page 13, Final Report Volume 1, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf

[17] See sections 736, 992AA and 992A

Case study 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

If the advice of the Australian Government is to *not* hand over log in details, it is inconsistent and dangerous to allow Australian FinTech companies to ask for and receive log in details to highly sensitive bank accounts.

Screen scraping breaches bank terms and/or conditions, whereby losing E-payments Code protection

Providing access to one's banking data using screen scraping technology amounts to a breach of the terms and conditions of a customer's bank account, and places customers at risk of losing their protections under the E-Payments Code.

The E-payments Code states:

> *11.2 Where a subscriber can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the pass code security requirements in clause 12: (a) the holder is liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of pass code security is reported to the subscriber*

The rationale for this is clear. Sharing a password is as detailed above, an inherently unsafe practice and it would be a moral hazard to allow consumers to provide such details and not be liable for the loss that occurs as a result.

Banking Terms and conditions make it very clear that providing a password to a third party breaches the terms and conditions of the facility. For example ME Bank states:

> *Account aggregation services – warning*
>
> *6.31 Some companies provide an account aggregation service that allows consumers to view account information from different institutions on the one web page. To use an account*

aggregation service, you are usually required to give the service provider your account details and your access codes (for example, your username and password and/or PIN).

6.32 We do not endorse or authorise the use of account aggregation services in connection with your account

6.33 Please remember that if you break your agreement with us not to disclose your PIN to another person, you will be liable for any transactions on your account made using your PIN. There is also a risk that information about your account obtained by an account aggregation service provider or its employees may be misused.[18]

FinTech Australia has however argued that rather than prohibiting the unsafe practice of screen scraping, the e-Payments Code itself should be updated to make it clear that customers are not liable for monetary losses, where they supply their passcode to a company accredited by ASIC.

> *Working closely with stakeholders to develop agreed passcode security and complaints handling standards, which is expected to legitimise existing industry safeguards and inform the ASIC accreditation approach.*[19]

There are a number of fundamental problems with this suggestion.

First encouraging people to hand over passwords and usernames runs counter to all other security advice provide by the Australian government as outlined above. Even if it was safe to hand over log-in details in the Fin Tech context – which it is isn't – it would undermine safe practices in all other online contexts.

And second accrediting screen scraping by ASIC undermines the entire point of the accreditation system under the Consumer Data Right regime.

The government's Consumer Data Right was developed for this very purpose. It is nonsensical to develop a parallel system to serve the interests of a small number of legacy FinTechs who are unwilling to change their business model to meet the higher standards and security requirements of the CDR regime.

Screen scraping is slow, unstable and prone to errors

In addition to being unsafe screen scraping is generally considered slow, with estimates that what would take 5 to 10 minutes to undertake via screen scraping takes seconds under Open Banking.[20] FinTech Australia also acknowledges that there are faster technological solutions available.

---

[18] Pages 18-19 Everyday Transaction Account Terms and Conditions https://www.mebank.com.au/getmedia/c0bf2e3a-30a3-492c-9690-c5397dc0a486/eta_terms_and_conditions.pdf

[19] Submission to Open Banking Inquiry, September 2017 https://treasury.gov.au/sites/default/files/2019-03/c2017-t224510_FinTech_2.pdf

[20] Kelly Read-Parish, Open Banking vs. Screen Scraping: looking ahead in 2019, 4 January 2019 https://www.finextra.com/blogposting/16494/open-banking-vs-screen-scraping-looking-ahead-in-2019

Furthermore screen scraping is fundamentally unstable and technology breaks down regularly. 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. Open banking APIs do not have this issue.

Case study 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.

Financial Rights has begun representing Gavin but upon looking at the data aggregation provided for responsible lending purposes, it was riddled with errors – including categorizing his café payments for coffee as rent.

Source: Financial Rights Legal Centre

Allowing screen scraping to continue undermines the potential success of the Consumer Data Right

There are advantages to both consumers and to financial services and FinTech companies in using third party providers to obtain bank statement information including the ease and speed of providing bank statement information for responsible lending and other appropriate purposes.

However this is very the reason the government's Consumer Data Right was established – to provide a fast, safe, and secure process to access personal and financial data.

The Consumer Data Right is fundamentally a right to port and transfer one's own personal financial data – similar to screen scraping – but in a safe environment "ensuring …high levels of privacy protection and information security for customer data"[21]

Without a ban on screen-scraping, there is very little incentive for businesses such as payday lenders and debt management firms to use CDR accredited software over screen scraping technology.

FinTech Australia have stated that:

> *"many fintech companies are happy with existing screen scraping solutions, and are likely to continue to use these solutions even when alternative technology is available."*

[21] The Hon. Scott Morrison, Treasurer, Media Release *More power in the hands of consumers*, 21 September 2018, http://sjm.ministers.treasury.gov.au/media-release/087-2018/

Joining the CDR regime involves justifiable higher regulatory hurdles, obligations and costs to ensure that consumers can have trust and confidence in those who they are sharing their sensitive financial data with.

Allowing the practice of screen scraping to continue therefore encourages those who seek to access financial data not to join the CDR – particularly those who may not meet the fit and proper person test under the accreditation regime, those who may not wish to spend the money (approximately $50,000 -$100,000) on gaining and maintaining accreditation[22] or those who see no reason to have to do so.

It has been suggested that FinTechs will naturally want to become accredited in order to gain the confidence of their potential users. While there are many service providers, for example, who may seek reputational legitimacy, many will not. Additional hurdles, regulations, obligations and costs introduced by an accreditation process will remain unattractive to many of these businesses, some of whom already skirt the regulations currently in place.

If the prevalence of irresponsible lending in the payday lending market is anything to go by, there is arguably little financial, reputational or other incentive for many FinTech players to seek accreditation if they can continue relying on old technology – even if it is riddled with problems.

Financially vulnerable people desperate to access credit via a service that uses old and unsafe screen scraping technology will not concern themselves with the nuances of privacy protections to do so. If that means engaging with non-CDR-accredited third parties like dodgy payday loan operators still using screen scraping, those financially vulnerable people will do so and end up with lower privacy protections than customers seeking loans from CDR accredited lenders.

Personal responsibility is commonly brought up as an argument to maintain the ability for consumers to choose to use services that use screen scraping technologies. But when consumers are excluded from accessing mainstream credit and the only provider will use screen scraping technology – there is no true choice here for a consumer to decide between obtaining credit and giving up privacy and other rights. Genuine consent is absent where the power is held by the provider.

Even non-financially vulnerable consumers may hold misplaced trust in a financial advisor or accountant who uses screen-scraping technologies. Indeed there is significant research that trust increases when a financial advisor provides information on conflicts of interest because the consumer believes they are being transparent and is therefore more deserving of trust.[23] The same principle could very well apply with respect to greater disclosure and transparency with respect to the application or lack of privacy safeguards. If the scandals in financial advice,

---

[22] Page 9, Senate Select Committee On Financial Technology And Regulatory Technology Issues Paper, https://www.aph.gov.au/~/media/Committees/fintech_cttee/Issues%20Paper%20-%20FinTech.pdf?la=en

[23] James Lacko and Janis Pappalardo, *The effect of mortgage broker compensation disclosures on consumers and competition: A controlled experiment*, *Federal Trade Commission Bureau of Economics Staff Report*, 2008 referenced in Financial Services Authority, Financial Capability: A Behavioural Economics Perspective, 2008: *"Even if the disclosure is noticed by consumers, it may have the effect of increasing trust in advisers rather than making consumers more wary."*

mortgage and insurance broking that led to the Financial Services Royal Commission are anything to go by, this will continue to be the case.

Two very distinct FinTech sectors will be created: a sector that will adhere to higher privacy safeguards and standards and a sector that will not.

This ultimately undermines the potential success of the CDR regime to ensure great consumer protections and increase confidence in the sector.

Allowing screen scraping to continue places Australian FinTech at a disadvantage

Screen scraping is a near defunct technology that the rest of the world is moving beyond.

Screen scraping has been banned in the UK and the EU under the Payment Services Directive 2 (**PSD2**). There is currently a 6 month transition ending 14 March 2020.[24]

The reasons for this are essentially to ensure UK customers are provided with safer and strong authentication processes under Open Banking. Screen scraping technology has been accepted as yesterday's technology and encouraging the Australian sector to continue to use the technology in the face of our own Open Banking system will place our industry at a disadvantage internationally as resources keep being poured into a defunct and out of date standard.

Banning screen-scraping will enable FinTech sector to develop consumer trust

Like all sectors of the financial services industry – and indeed the broader economy - the FinTech sector will thrive or remain stunted on the basis of consumer confidence in the products and services they provide. The FinTech sector though is particularly vulnerable to the threats borne of the nature of their offering – that is the potential for their services to be and be seen to be unsafe, insecure, manipulative or downright dangerous.

It is therefore in the sector's interest and the Australian economy's interest to build a safe and secure, forward thinking regulatory environment that promotes consumer confidence and engagement. Banning screen-scraping is fundamental to this transformation.

Recommendations

8. **The Inquiry should recommend that screen scraping be prohibited to support the success of the Consumer Data Right regime.**

[24] FCA, Strong Customer Authentication, 2 September 2019, https://www.fca.org.uk/firms/strong-customer-authentication