



**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, September 2019

December 2019

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 Senate Select Committee on Financial Technology and Regulatory Technology's inquiry into Financial Technology and Regulatory Technology. Our submission will be focussed on the FinTech sector.

The committee notes it is seeking input on whether regulatory settings support the growth of FinTech companies in Australia. We believe that the more important question is whether regulatory settings support positive outcomes for consumers and that this should be the primary focus when examining the regulatory settings governing the FinTech sector.

While we support the development of innovative services and business models that meet the needs of consumers, we are concerned about the potential risks to consumers of some forms of innovation. Given the capacity for business models to be created and adapt to avoid regulation, it is our view that much of the existing legal and regulatory frameworks are no longer fit for purpose. The result of this is that many consumers, particularly those experiencing vulnerability or disadvantage, either do not benefit or suffer detriment from a quickly evolving marketplace.

The framing of this Inquiry fails to consider these risks and appropriate regulatory responses for Fintech industries. In recent years we have witnessed small and large financial service providers demonstrate appallingly low regard for consumer needs and protections including through the misconduct identified in the Financial Services Royal Commission. We are concerned that providers invoking a halo of 'innovation' may fall through the gaps of consumer protection requirements. For this reason, we consider that robust regulatory protections need to be built into any framework that seeks to support the development of Fintech. Consumer protections must be in place and regulators properly resourced to keep up with a fast-moving industry with rapid uptake and potential for wide-spread consumer harm to result.

The premise that barriers exist that are preventing this industry from growing is misguided. Rather than framing this industry as 'opportunity' that faces barriers to greater 'uptake' this inquiry should consider how technologies can tangibly improve the lives of Australians. Legislative or regulatory requirements exist to protect people and the Committee should be cautious of companies that seek to exploit loopholes in existing laws or regulation. As noted in Australia's competition legislation and in recent reviews of competition settings, competition is a means to achieve good consumer outcomes and not an end in itself.¹

This submission puts forward the view that for the FinTech sectors to flourish and grow, consumers must have confidence that their engagement with their products services and innovations are safe, secure and will not lead to consumer harm. Australian consumers are rightfully wary of the digital economy and current data practices. In a groundbreaking consumer survey, the Consumer Policy Research Centre found that:

¹ Australian Government – The Treasury, *Competition Policy Review – Final Report*, 31 March 2015, available at: <https://treasury.gov.au/publication/p2015-cpr-final-report>

- Ninety-five per cent wanted companies to give options to opt out of certain types of information collected about them, how it can be used and/or what can be shared with others
- Two-thirds (67 per cent) indicated that they still signed up for one or more products even though they did not feel comfortable
- The most common reason (73 per cent) for accepting privacy policies with which consumers were not comfortable was that it was the only way to access the product or service;
- Consumers surveyed found it unacceptable for companies to:
 - Charge different consumers different prices based on their (data) profile (88 per cent)
 - Collect data about them without their knowledge to assess eligibility or exclude from a loan or insurance (87 per cent)
 - Use payment behaviour data to exclude from certain essential products and services (82 per cent)
- Seventy-three per cent believe Government should ensure companies give consumers options to opt out of what data they provide, how it can be used and if it can be shared
- Sixty-seven per cent believe Government should develop protections to ensure consumers are not unfairly excluded from essential products or services based on the data or profile.

A strong regulatory environment is required to ensure FinTech innovation is sustainable and in line with consumer and community expectations through:

- building consumer trust and confidence in the FinTech sector;
- empowering consumer by providing them with genuine choice and control over collection, sharing and use; and
- Ensuring consumer right to privacy is adequately protected.

This submission puts forward a number of reform recommendations to lead the FinTech to such an environment. These are:

- Improve consumer protections under the Consumer Data Right;
- Modernise the Australian Privacy Act;
- Prohibit the dangerous practice of screen scraping;
- Develop a legally enforceable AI Ethical Framework;
- Prohibit unfair trading practices; and
- Regulate Buy Now, Pay Later services.

Improve consumer protections under the Consumer Data Right

Our organisations have made multiple submissions to the development of the Consumer Data Right (CDR) outlining our concerns with the regime – in particular with respect to its approach to consumer protections.

The CDR will be introduced into the banking sector in phases, with data relating to personal and business accounts becoming available from February 2020. Following the passing of legislation, the ACCC has developed draft set of CDR Rules and CSIRO's Data 61 are working on developing the Consumer Data Standards – the development of common technical standards to allow Australians to access data held about them by businesses and direct its safe transfer to others.

Financial Rights has attended a number of workshops on the consumer experience of the CDR. The consumer voice was seriously under-represented in the development of consumer experience standards, with there often being only one or two consumer advocates in the room compared to over 40 industry participants.

More significantly though, we have been concerned with the approach many FinTechs are taking to the CDR standards and the rules. Much of the work that we witnessed in these workshops has been directed at ways FinTech's can get around rules that have been set including:

- 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 including the use of 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 many examples of this:

- One FinTech representative stated that they had figured out a loophole to the CDR regime where unaccredited FinTechs² can simply ask for people to hand over the data that the consumers themselves request directly from their data holder in a machine readable format. These FinTechs/companies would therefore not have to get accredited. This is in fact the issue that the consumer movement has been warning about in the development of the CDR rules and legislation – leakage of sensitive financial data outside of the protections of the CDR framework. 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. This fundamentally undermines the concept of consent as detailed under the rules ie voluntary, express, informed, specific as to purpose etc. Will people really be freely

² Or the clients of Fintechs using their services

consenting to a particular use if that consent is based on an incentive unrelated to the use. There is currently nothing in the Draft Rules to prevent Accredited Data Recipients providing CDR Consumers with a reward or incentive if they provide their consent for the Accredited Data Recipient to de-identify some or all of the collected CDR Data for the purposes of disclosing (including by selling) the de-identified data (in accordance with Rule 4.11(3)(e)).

- As an example of designing the consumer experience to benefit the FinTech over the interests of the consumer, FinTech representatives wanted to obfuscate the consumer's choice in the design of the re-authorisation process. Consumers will at some point need to either re-authorise a FinTech App or cease use of the app. FinTech representatives asserted that the clearest way to ask a consumer whether the consumer wanted to re-authorise something was to provide them with 2 choices: "Modify" or "More info". Not simply "Re-authorise" or "Stop sharing data" (or simply "delete."). This obfuscation is clearly in the interests of the industry rather than the consumer. At every opportunity the FinTech sector representatives sought to build in "friction" to the process of deleting one's data. This seeking of increased "friction" in this case is somewhat ironic given the relentless calls from the FinTech sector to make the CDR, data-sharing and switching "frictionless" transactions. It is only where the Fin Tech sector's self-interest is served, in seeking to hold onto customers and their data, that they see the benefits of friction.

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 and amend and improve the standards and recommend changes to the governing legislation, when and where FinTech arbitrage leads to demonstrably poor consumer outcomes.

We note that Treasury engaged Maddocks to prepare an iteration of the CDR's Privacy Impact Assessment (**PIA**) to identify the impacts that the CDR may have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating these impacts. This report detailed significant issues with the current CDR – many of which reflect our organisation's previously expressed concerns.

The PIA then makes a series of recommendations to improve consumer protections. The Treasury and other responsible agencies have responded to the recommendations set out by Maddocks in the PIA.

We note that Treasury and other responsible agencies have supported many of the recommendations. We support the regulators implementing these recommendations as soon as possible.

However the response has failed to address other fundamental issues with the CDR regime including the issue alluded to above that, if the CDR Consumer provides their CDR Data that it has received from a Data Holder, to a third party, the privacy protections afforded to that CDR Data under the CDR regime will not apply.

One of the key aims of the CDR is to create a safe and secure environment in which consumers will be able to trust and have confidence that they will be able to transfer or port their data from one data holder or participant to another. However the CDR legislation will facilitate non-

accredited parties obtaining CDR information, leaving these consumers, who were led into a system on the promise of higher privacy protections, vulnerable to the lower privacy standards of the APPs.

We strongly believe that legislative change will be required to address these risks. They include:

- amending the Privacy Act and the APPs to ensure that the same strong protections under the CDR apply to all consumer data;
- requiring any entity handling CDR Data (including Data Holders) to be accredited in a similar manner to accreditation of Accredited Data Recipients;
- ensuring third party recipients have clear obligations about the handling of CDR Data they receive by, for example, extending the application of the Privacy Safeguards to apply to third party data recipients of CDR Data; and/or
- banning screen-scraping and similar unsafe data access, transfer and handling technologies.

Another reform that would deal with many of the issues is moving the Data Standards being developed from a mix of non-binding and binding requirements to binding requirements. The distinction between binding and nonbinding standards inevitably leads to the regulatory arbitrage described above and provides significant scope to the FinTech industry to design interfaces that serve themselves well, and serve consumers poorly. We therefore recommend that rather than merely distinguishing between binding and non-binding requirements – that all guidelines be binding and enforceable.

Recommendations

1. The Inquiry should endorse recommendations of the CDR Privacy Impact Assessment and recommend that the regulators implement the recommendations in full and as soon as possible.
 2. The Inquiry should recommend:
 - a) amending the Privacy Act and the APPs to ensure that the same strong protections under the CDR apply to all consumer data;
 - b) requiring any entity handling CDR Data (including Data Holders) to be accredited in a similar manner to accreditation of Accredited Data Recipients;
 - c) ensuring third party recipients have clear obligations about the handling of CDR Data they receive by, for example, extending the application of the Privacy Safeguards to apply to third party data recipients of CDR Data; and/or
 - d) banning screen-scraping and similar unsafe data access, transfer and handling technologies.
 - e) Ensuring that all CDR standards are binding upon participants.
-

Modernise the Australian Privacy Act

We strongly support broader reform of the Australian privacy regime to better promote and support the interests of consumers by placing their interest front and centre of the regime over the profit-driven interests of FinTechs, digital platforms and businesses to retain, use and exploit private information.

We note the Government's response to the Digital Platform Inquiry includes the announcement of 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..."

The review will consider a number of ACCC recommendations that the Government has supported in principle including:

- updating the "personal information" definition: Recommendation 16(a);
- strengthen notification requirements: Recommendation 16(b);
- strengthen consent requirements and pro-consumer defaults: Recommendation 16(c);
- enable the erasure of personal information: Recommendation 16(d),
- introduce direct rights of action for individuals: Recommendation 16(e), and
- increase penalties for breaches: Recommendation 16(f).
- introduce a statutory tort for serious invasions of privacy: Recommendation 19.

If consumers are to have any trust in digital commerce moving into the future, these broader reforms are essential.

As the Government has stated:

Data is the resource that powers much of this activity, and it is being created and collated at an unprecedented scale. The capacity to process this data is also improving, providing us with greater insights and information than ever before.

While the benefits of digital services and technology are vast and will continue to grow, we must also be aware of, and respond appropriately to, the risks that are presented so that consumers and businesses have the confidence and capacity to engage in the digital world.

We recommend that this inquiry not undertake its work in a vacuum and support the application of stronger privacy laws and other mooted reforms to the FinTech sector.

Recommendations

3. The Inquiry endorse and support the need to review and strengthen the Privacy Act to ensure consumers and businesses have the confidence and capacity to engage in the digital world.
-

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."*³

The Australian Government's StaySmartOnline website states:

*"Keep your passwords secure by taking measures to protect them: Don't share your passwords with anyone."*⁴

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*⁵

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.⁶

Case study Zed's story

Zed (name changed) 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.

³ <https://www.moneysmart.gov.au/scams/avoiding-scams>

⁴ <https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/passwords-business>

⁵ <https://my.gov.au/mygov/content/html/security.html>

⁶ We note that FinTech Australia report that "between 10-50 per cent of potential customers balk at handing 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.

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.”⁷ 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*⁸ 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:

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. The lender refused to rescind the

⁷ 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>

⁸ See sections 736, 992AA and 992A

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.⁹

⁹ 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

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.¹⁰

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.¹¹ FinTech Australia also acknowledges that there are faster technological solutions available.

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.

¹⁰ Submission to Open Banking Inquiry, September 2017
https://treasury.gov.au/sites/default/files/2019-03/c2017-t224510_FinTech_2.pdf

¹¹ 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>

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”¹²

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.”

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

¹² 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/>

(approximately \$50,000 - \$100,000) on gaining and maintaining accreditation¹³ 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 entities 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.¹⁴ 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, 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.

¹³ 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

¹⁴ 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.”

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 2020.¹⁵

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

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

¹⁵ FCA, Strong Customer Authentication, 2 September 2019, <https://www.fca.org.uk/firms/strong-customer-authentication>

Develop a legally enforceable AI Ethical Framework

In order to support an appropriate regulatory regime for FinTech companies to achieve positive outcomes for consumers then the Committee must put ethical questions around technology, innovation and data front and centre of this consideration. This is particularly the case with respect to the use of Artificial Intelligence in FinTech.

Financial services and Artificial Intelligence

In the financial services sector new computing power and technology has led to:

- an expansion of the data collection from their own customers as well as from external sources both conventional (e.g. government databases and transactional data), and unconventional (e.g. social media, emails etc.);
- advanced data processing techniques; and
- advanced analytical, artificial intelligence and algorithmic techniques including predictive analytics.

AI is consequently well suited to exploitation in the financial services sector given AI's ability to recognise patterns, predictively anticipate future events based on large sets of data and make decisions based on this information. The example above of payday lenders hawking loans to individuals when it detects low bank balances is evidence of this.

The burgeoning FinTech sector is creating products, services and tools that are transforming ways the sector undertakes risk assessment, detects and manages fraud and assists consumer manage their finances.

New and emerging services involving some element of AI technologies include:

- new services embedded in mobile and online banking;
- Open Banking applications using consumer transaction data to assist in a series of services including but not limited to account switching, mortgage search services;
- new personal financial management services (such as Money Dashboard);
- investment and wealth management services with automated or robo-advisers services such as Wealthfront;
- new lending and unsecured credit services based on data led credit-scoring and risk profiling (e.g. Afterpay, Defer It);
- encrypted digital wallets that store bank, debit or credit card detailing for online payments (e.g. PayPal and AliPay);
- neo banks and FinTech savings banks such as AliPay's Yu'eBao;
- offline mobile payments such as Apple Pay, Android Pat or Ali Pay used at retail locations; and

- credit scoring and social scoring – utilising financial and social datasets from non-traditional sources such as Facebook and other social media to create measures of credit worthiness, outside of the “traditional” credit reporting and scoring.

There is also a sub-class of FinTech known as insurance technology or InsurTech. InsurTech is using AI technologies in three key ways.

Firstly it is using AI to build behaviour into premium pricing. Connected devices and telematics technology (e.g. Fitbit), connected home technologies (e.g. Amazon Alexa) and what is known as the “Internet of Things” (e.g. connected smoke alarms, locks, fridges and light switches) are also being put to specific use by the insurance sector.

Telematics technologies involve the use of GPS technology and increased information processing power to collect and transmit information and data to insurers directly. Telematics devices being used by insurers include:

- Motor vehicle telematics – devices in vehicles that can record GPS location data as well as information from a vehicle’s engine management system to monitor all aspects of driving style. QBE, for example, offers “Insurance Box for young drivers”. Here, drivers install an electronic device or “black box” in their car that transmits back to the insurer a detailed breakdown of their driving habits in areas such as their braking, acceleration, steering, cornering, speed and night driving.¹⁶ QBE then calculate a “DriveScore” rating to evaluate the driver. The higher the DriveScore the less the policyholder will pay for insurance. The lower the score, the more the driver pays.
- Home telematics – devices can monitor the use and supply of a range of utilities as well as security of a home. Smart smoke alarms, water leak and freeze detectors are already being used overseas by insurers.
- Health monitors – fitness monitors such as Apple Watch and FitBit can record the location, movement, activities and other health information. AIA vitality¹⁷ is an example of a product that enables a life insured to gain benefits such as discounts and rewards via the earning of “vitality points” for activities undertaken.¹⁸ Others include Asteron Life Plus Health Rewards and Bupa Living Well.

Life insurers are using genetic testing technology in their underwriting provided to them under disclosure laws, an ability borne of increased computing processing power, new hardware and data analytics.

AI is also being used in insurance to personalise the customer experience through the use of chatbots and other tools to improve the sales experience.

And finally AI is being used to ‘enhance’ the claims handling process including fraud detection through data analysis and machine learning, and speeding up the settling of claims. Many of the FinTech and InsurTech services are using algorithms and AI for automated decision making,

¹⁶ <https://www.qbe.com.au/news/car/how-insurance-box-works>

¹⁷ <https://www.aiavitality.com.au>

¹⁸ <https://www.aiavitality.com.au/vmp-au/rewards>

sometimes with adverse outcomes.¹⁹ Developing an enforceable AI ethical framework will assist in driving positive outcomes for consumers.

Ethical implications of the use of AI in financial services

FinTech products and services' utility arises from a near total reliance on data – largely a consumer's personal financial data - their transactions history, credit history, biometrics etc. FinTechs and InsurTechs are also integrating financial data with other data about individuals drawn from social media and other sources – information that people would consider have nothing to do with their financial status. InsurTech is tracking people's every movement and drawing conclusions about a person's identity and their life derived from the use of their car.

This increased collection of data is feeding the creation of a “financial identity” – a concept increasingly used by financial institutions to take user data and make assumptions based on that.

Financial institutions have for years stored and verified customer identities and attributes through “Know Your Customer” systems i.e. the process by which banks or other financial institutions identify their customers in order to evaluate the possible legal and other risks. They therefore have a commercial incentive to collect more and more accurate information about their individual customers. The World Economic Forum in 2016 has in fact argued that financial institutions “should champion efforts to build digital identity systems, driving the building and implementation of identity platforms.”²⁰

However the development of an increasingly accurate financial identity built by data has serious consequences for consumers.

Some positive impacts include enabling increased access to financial services and potentially empowering consumers in increasing their own financial literacy, behaviour or wellbeing.

There are however a series of impacts upon consumers – particularly consumers experiencing financial vulnerability or hardship - that are of significant concern to Financial Rights. We detail the following identified harms. While some of these cleave to ethical issues already raised in the Discussion Paper, there are new and further dimensions that we believe need to be considered in developing an Ethical Framework.

Profiling for profit: Increased economic inequality and financial exclusion

Financial Rights is concerned that with the rise of AI in FinTech, we will see increased occurrences of consumers being 'profiled for profit', which will see more people experiencing financial difficulties being offered unsuitable (but highly profitable) products. Or excluded

¹⁹ For example, a media report in the UK claimed that drivers were charged significantly different amounts based on their name: <https://www.newstatesman.com/politics/uk/2018/01/higher-insurance-if-you-re-called-mohammed-s-just-start-institutionalised>

²⁰ World Economic Forum & Deloitte (2016) “A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity”: page 28
http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Target marketing of products to particular groups of consumers is not new. In consumer lending, technology can be used to identify consumers who are likely to be profitable, tailor and price products that the most profitable customers are likely to accept, and develop strategies to reduce the likelihood that the most profitable customers will close their accounts.

Consumers struggling with debt are often the most profitable customers for banks and lenders. It is often argued that it is not in the interests of lenders to extend credit to people who are unable to repay. However, our experience suggests that many consumers struggle for years at a time to make repayments to their credit accounts without ever reaching the point of default, but paying significant amounts of interest. These customers are very profitable for lenders, despite the fact that repayments can result in further financial hardship.

We have seen other highly risky and harmful 'Fintechs' such as contracts-for-difference providers engage in regulatory arbitrage in the past, where Australia has been seen as a soft target and used as a regulatory base for predatory investment platforms.²¹

What is of more significant concern is that with the automating of these processes through an Open Banking regime and the application of AI to this, there will be significant room for increased exploitation. Consumer advocates in the United Kingdom, have already raised concerns that 'Open Banking enables lenders to continually monitor accounts and take repayment as soon as income is detected'²². These are real risks that are poorly understood by consumers and unlikely to be dealt with by disclosure and consent because of the take it or leave nature of the service.

Price discrimination on low-income households

Much of the promise of FinTech is that more tailored products and services will be made available with lower fees or lower loan interest rates for many banking customers. However, the flip side to lower fees and interest rates for some is that costs will increase for others. These 'others' will undoubtedly be Australia's most vulnerable, disadvantaged and financially stressed households.

Those in more precarious financial situations – again identified as such by their data driven financial identities - will likely be unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders. In other words, the consumers who can afford it the least will pay the most be it via higher interest rates or higher fee products. There are serious fairness considerations at play here. As banks and credit providers are increasingly able to use consumer data and technology to better automate the targeting of particular financial services offers to profitable consumers, we will likely see an increased use of 'risk-based pricing'. This may result in some lenders targeting 'riskier' borrowers with higher interest rates. While risk

²¹ Australian Financial Review, *CFD players accused of 'regulatory arbitrage'*, 22 August 2019, <https://www.afr.com/companies/financial-services/asic-to-ban-retail-2b-in-risky-derivatives-20190822-p52jkt>

²² Open Banking, A Consumer Perspective, Faith Reynolds, January 2017 <http://docplayer.net/39177571-Open-banking-a-consumer-perspective-faith-reynolds.html>

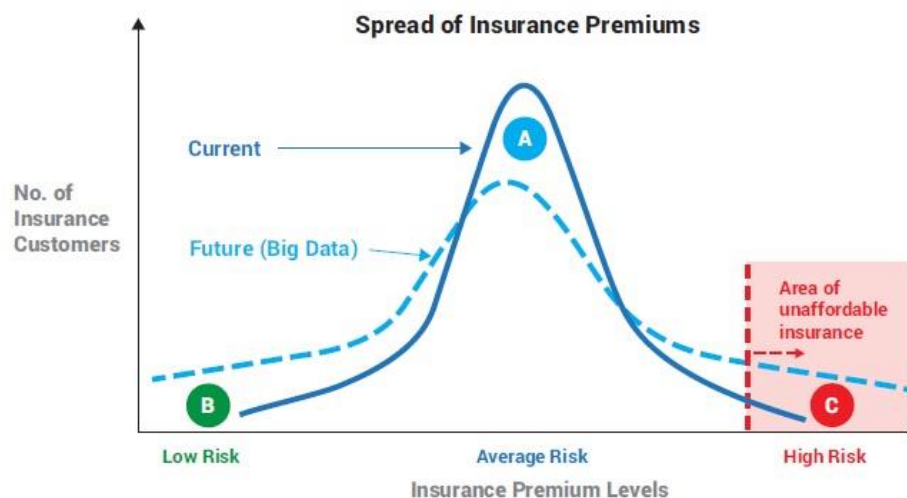
based pricing has effectively existed in Australia in the non-bank sector for some years, it is now moving into mainstream banking.

A 2015 report by United States organisation Data Justice raised concerns that enabling advertisers to offer goods at different prices to different people to extract the maximum price from each individual consumer. The report found that such price discrimination not only raised prices overall for consumers, but particularly hurts low-income and less technologically savvy households.²³ In fact, the ability to segment the market further will likely mean that firms can 'cherry pick' the most commercially viable consumers and exclude others (or charge them more).²⁴

It is clear that the result of the price discrimination in credit enabled by these technologies in the financial services sector is a downward spiral of debt. A self-fulfilling prophecy ensues. A consumer's low credit rating decreases from a default, which in turn feeds an algorithm of credit-worthiness leading to higher interest rates and further financial difficulty and further defaults.

In the insurance sector, the increased use of big data analysis and automated processing allowed by increased computing power will enable insurers to increasingly distinguish between risks on an increasingly granular level. This will lead to the higher risks only being able to be insured for higher prices or on worse terms. According to the Actuaries Institute

At the extreme, some policyholders will have their risks assessed as so high that the price will be prohibitive or insurers will decline to provide cover. The following diagram illustrates the effect that increasing data will have on insurance premiums.



Overall, there will be fewer insureds treated as "average" risk (area A) and paying average premiums. They will increasingly be classed as either lower or higher than average. Greater

²³ Data Justice, Data Justice Report: Taking on Big Data as an Economic Justice Issue, 2 October 2015, available at: <http://www.datajustice.org/blog/data-justice-report-taking-big-data-economic-justice-issue>

²⁴ 7 Faith Reynolds, Open Banking: A Consumer Perspective, January 2017, p. 23, available at: <https://home.barclays/content/dam/home-barclays/documents/citizenship/access-to-financial-and-digital-empowerment/Open-Banking-A-Consumer-Perspective-Faith-Reynolds.pdf>

numbers of insureds will thus be recognised as being lower risk and given lower insurance premiums (area B). Conversely there will be more consumers falling into the higher risk category, ultimately reaching the “unaffordable” levels of insurance premiums (area C).

...

In response, some people may mitigate or avoid the risk. Others who find the insurance premiums for their risk to be unaffordable may have to take the risk themselves. If the risk event does happen, they will suffer financially. The more people change from insured to uninsured status because of price increases arising from more targeted use of data, the greater the burden will be on the public purse or on others outside the insurance system.²⁵

Unfair and exclusionary price discrimination practices in insurance and the broader financial services sector should be a cause for serious concern where it contributes to lower-income people paying higher prices than others, or where pricing discrimination negatively affects particularly marginalised groups. In the insurance sector, people who need insurance the most may increasingly find they have been excluded completely as a result of issues which may be completely beyond their control. These are key issues of fairness and equity which this Committee should consider and address. Such exclusion also flies in the face of government efforts to increase financial resilience, and ultimately puts pressure back on the government and community to pick up the pieces where the market has failed and those affected are in no position to cover their own losses.

Indirect Discrimination

Algorithmic decision making in the financial services sector has great potential to introduce bias into decision making particularly for marginalised consumers.

Researchers have pointed to a “system in which power over the judicious and ethical use of data is overwhelmingly concentrated among white men” resulting in negative consequences for minority groups.²⁶ This is because unconscious biases that are held by an individual or group of individuals becomes part of the technology that they create. Questions around what data should be collected, how it is used and who is making these decisions need to be interrogated.

Closed proprietary algorithms used by FinTechs and InsurTechs to automatically calculate an individual’s credit worthiness or the interest rate they are offered could also potentially lead to situations where consumers are denied access to crucial products and services based on accurate or inaccurate data without the ability to determine why or to correct underlying assumptions.

Algorithmic bias or discrimination is already well documented²⁷ and arises when an algorithm used in a piece of technology – say a FinTech product or service – that reflects the implicit or

²⁵ Page 19-20, Actuaries Institute, The Impact of Big Data on the Future of Insurance <https://actuaries.asn.au/Library/Opinion/2016/BIGDATAGPWEB.pdf>

²⁶ <https://theconversation.com/data-ethics-is-more-than-just-what-we-do-with-data-its-also-about-whos-doing-it-98010>

²⁷ See Cathy O’Neil, Weapons of Math Destruction, 2017

explicit values of those who are involved in coding, collecting, selecting, or using data to establish and develop an algorithm.

Credit scoring, social scoring or e-scoring algorithms for example can produce feedback loops where somebody from a particular suburb where a lot of people default can be given lower credit ratings due to that association, or where a particular address is charged a higher premium based on the habits and attributes of previous occupants – an example that a client of Financial Rights experienced. Statistical correlations used by actuaries between a person’s postcode (here geographical information standing in for a particular race, ethnicity or culture); their language patterns on social media; their potential to pay back a loan; or, keep a job; can lead to significant discrimination being built into opaque black box algorithm technology.

Cybercrime, identity theft and material theft

As our financial services sector becomes more and more reliant on technology with greater access to accurate personal information– the fuel on which AI depends – individuals become increasingly vulnerable to cybercrime.

Firstly consumers are vulnerable to identity theft. With increasingly sensitive and accurate data being held by FinTechs, breaches of these datasets make it easier for criminals to use this identifying information to undertake subsequent crimes, financial or otherwise.

The vulnerability of the data protection systems in place also facilitates actual theft of property – that is the hacking of FinTech systems to access payment systems and steal money. According to Juniper Research, fraudulent online transactions will reach a value of \$25.6 billion by 2020²⁸ In Australia online credit card fraud, with transactions made using stolen card details hitting \$417.6 million in 2016, more than doubling since 2011.²⁹

The news³⁰ that UK company Cambridge Analytica legitimately gathered some personal data from Facebook accounts and concurrently illegitimately gathered other people’s data, and then, when found out and were requested to delete the data, did not, has raised public consciousness over the potential for data to be misused in various ways. Combined with the never-ending list of significant and high profile data breaches at Equifax, Ashley Madison, Yahoo and more, consumer awareness of how vulnerable consumers are is increasing every day.

²⁸ “Online Transaction Fraud to More than Double to \$25BN by 2020’ Juniper Research UK, May 2016.

²⁹ Lucy Cormack, Carol Saffer, Online credit card fraud on the rise, accounting for 78 per cent of total card fraud in Australia, SMH, 3 August 2017 <https://www.smh.com.au/business/consumer-affairs/online-credit-card-fraud-on-the-rise-accounting-for-78-per-cent-of-total-card-fraud-in-australia-20170802-gxnwd7.html>

³⁰ ‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower, *The Guardian*, 18 March 2018 <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

A legally enforceable AI Ethics Framework is required

This Inquiry presents an opportunity to help embed principles within the FinTech sector that ensure they promote ethical value creation rather than value appropriation.

The Department of Industry, Innovation and Science recently developed a set of voluntary principles that are designed to be used when designing, developing, integrating or using artificial intelligence (AI) systems.³¹

The eight principles are:

- *Human, social and environmental wellbeing: Throughout their lifecycle, AI systems should benefit individuals, society and the environment.*
- *Human-centred values: Throughout their lifecycle, AI systems should respect human rights, diversity, and the autonomy of individuals.*
- *Fairness: Throughout their lifecycle, AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.*
- *Privacy protection and security: Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.*
- *Reliability and safety: Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose.*
- *Transparency and explainability: There should be transparency and responsible disclosure to ensure people know when they are being significantly impacted by an AI system, and can find out when an AI system is engaging with them.*
- *Contestability: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output of the AI system.*
- *Accountability: Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.*

The principles complement existing AI related regulations and are intended to:

- achieve better outcomes
- reduce the risk of negative impact
- encourage the highest standards of ethical business and good governance.³²

While the establishment of this voluntary framework is a good start it is clear that this will not be enough moving into the future. As the AHRC recently stated:

³¹ <https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles>

³² <https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles>

The Australian Government's AI Ethics Framework, outlined above, is an important, but modest, step that aims to prevent social harm associated with AI.³³

The voluntariness of the ethics framework means that there will be:

no rigorous, independent way of holding an individual or corporation to account in adhering to these principles, and no concrete consequences that flow from a failure to adhere. This is not inherently problematic. A voluntary commitment to abide by certain ethical principles can influence behaviour. A problem arises, however, if such voluntary commitments occupy the proper place of enforceable legal rules.³⁴

The AHRC has subsequently recommended that the government begin the process of moving towards the reification of ethical frameworks into the law.

Ethical frameworks can be important, but they cannot be a substitute for the law. This is as true amid the rise of new technologies, as it is in any other context. The Commission considers that there is a need to re-articulate the conventional relationship between the law and ethics in regulating behaviour.³⁵

The AHRC consequently propose that:

The Australian Government should commission an appropriate independent body to inquire into ethical frameworks for new and emerging technologies to:

- (a) assess the efficacy of existing ethical frameworks in protecting and promoting human rights*
- (b) identify opportunities to improve the operation of ethical frameworks, such as through consolidation or harmonisation of similar frameworks, and by giving special legal status to ethical frameworks that meet certain criteria.³⁶*

We agree that this would be an important first step.

Australia has the potential to foster a growing, high quality and consumer focussed Fintech industry -setting high minimum standards would provide a strong foundation. It would also prevent a regulatory 'race to the bottom' and a culture that seeks to undermine regulators or exploit loopholes.

We also believe that the FinTech sector could act now and agree to adhere to the AI Ethics Framework via a Code of Practice. Alternatively the ACCC CDR Rules should be amended to require CDR participants to meet these standards.

³³ Page 52, AHRC, Human Rights and Technology Discussion Paper
https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

³⁴ Page 54, AHRC, Human Rights and Technology Discussion Paper
https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

³⁵ Page 55, AHRC, Human Rights and Technology Discussion Paper
https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

³⁶ Proposal 2, Page 57, HRC, Human Rights and Technology Discussion Paper
https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

Recommendations

5. The Inquiry should support FinTech sector adhering to the AI Ethics Framework at least via a Code of Practice or under the ACCC CDR Rules.
 6. As the next step towards an enforceable ethical framework for AI, the Inquiry should support and endorse AHRC proposal 2.
-

Prohibit unfair trading practices

The Final Report of the Financial Services Royal Commission identified six norms of conduct, one of which was to ‘act fairly’.³⁷ The norm of fairness is also recognised in the objective of the *Competition and Consumer Act 2010* (Cth) which is ‘to enhance the welfare of Australians through the promotion of competition and *fair trading* and provision for consumer protection.’

Just as the concept of fairness must be applied in the “real world” financial services sector, the same must be applied to the FinTech sector.

Enacting an economy-wide prohibition on unfair trade practices as recommended by the ACCC in the Digital Platforms Inquiry will ensure fairer outcomes for consumer across the real world and digital economies.

This has been supported by Government who has backed the work of Consumer Affairs Australia and New Zealand on exploring how an unfair trading prohibition could be adopted in Australia to address potentially unfair business practices.³⁸

Unfair business models and practices are incessant

Consumer harm continues in the face of existing consumer protections. Harmful business models and practices persist and case law confirms that practices that are unfair may not be unlawful. Harmful business models and practices that are not strictly unlawful have already begun to emerge in the FinTech sector and the digital environment more broadly. Some of these have been outline above with respect to screen scraping practices and issues with respect the application of AI but also include:

- Services requiring provision of detailed personal information without a business or legitimate reason for that information, enabling the service to monetise that information through profiling, target marketing or on-selling;
- Subscription traps, which include business models that are free upfront or for an initial period, but terms and conditions require ongoing payment³⁹
- Services, memberships or marketing emails that make cancellation difficult, or employ deliberately confusing or tricky questions or processes to cancel.⁴⁰

³⁷ Royal Commission into Misconduct in the Banking, Finance and Superannuation Industry, Final Report, page 8.

³⁸ Regulating in the digital age Government Response and Implementation Roadmap for the Digital Platforms Inquiry, December 2019, <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf>

³⁹ See, e.g., <https://www.choice.com.au/shopping/online-shopping/buying-online/articles/beware-subscription-traps-warns-acc>

⁴⁰ See, e.g. Mathur et al, ‘Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites’, July 2019, available at: <https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns->

- Bundling products or services in such a way that prevents price comparison;⁴¹
- Charging loyal customers far more for the same product compared to new customers, without a legitimate justification or economic reason⁴²
- Marketing practices or product disclosures that do not include clear, upfront and timely information that may lead the purchaser into error; and
- Business models that target consumer vulnerabilities or behavioural biases, distorting the consumer's free choice

The operation of the free market in Australia has failed to deliver fair outcomes for everyone. The above list demonstrates this—the market has not prevented these substantive unfair practices from becoming widespread. Moreover, these unfair practices are more likely to impact disadvantaged or vulnerable groups. Consumers that are less savvy or less able to protect their own interests, for example due to factors like age, language, health or capacity, are more likely to experience detriment associated with unfair practices.

It is sometimes suggested that more effective competition will incentivise suppliers to meet customer needs. Effective competition is indeed an important discipline on business conduct. However, there is a real risk that competition without appropriate legal and regulatory safeguards can fail to deliver fair outcomes.

The DPI Final Report confirms problems with competition in the context of digital platforms, and market power held by the large digital platforms such as Facebook and Google. However, it is highly unlikely that more competition will deliver fairer outcomes. As identified by the ACCC, harmful practices relating to data collection (including location tracking, online tracking for targeted advertising purposes, and the disclosure of data to third parties) are common in businesses beyond the big digital platforms. The business incentives created by competition and free market orthodoxy serve to embed these practices of concern, rather than deliver on community expectations relating to fairness. It is for this reason that consumer law has a very important role to play.

Conceiving fairness: the scope of a provision on unfairness

An economy-wide provision prohibiting unfair trade practices should ensure that not only the practices of firms are fair in terms of the processes followed but in terms of the outcomes delivered. This would include, for example, the prices consumers pay. This supports a move towards outcomes-based regulation and a focus on good culture within firms. Such an approach

[v2.pdf](#) Page 15-16 includes a frustrating example: “Are you sure you want to cancel your membership” You will no longer receive membership pricing: click “continue” or “cancel”. Another example involves consumers choosing the buy now, pay later option at an online check out with no way to go back, effectively locking the consumer into the transaction.

⁴¹ See, e.g., <https://www.darkpatterns.org/types-of-dark-pattern/price-comparison-prevention>

⁴² See, e.g., Competition and Markets Authority, Loyalty Penalty Super-Complaint, available at: <https://www.gov.uk/cma-cases/loyalty-penalty-super-complaint>

can also mitigate harms associated with unequal outcomes among different classes of consumers in market, particularly consumers experiencing vulnerability.

This can be achieved through a simple principles-based provision prohibiting unfair trade practices, including practices that are likely to have an unfair outcome. The detail of the provision can be left to guidance from regulators about expectations of firms, as well as later interpretation of the courts. In this way, a prohibition on unfair trade practices can complement the other principles-based provisions in the ACL. To operate as a community norm, in both a preventative and remedial fashion, we consider it unnecessary for the scope of the provision to be restricted or limited in the legislation itself.

That said, it is helpful to conceive the scope of such a provision to understand its import and impact. In conceiving the scope of a provision prohibiting unfair trade practices, we consider that it is helpful to consider the life course of a consumer transaction or service in the FinTech context: covering sales and marketing; product/service design & pricing; as well as service elements, including post-sale customer service. It is also useful to draw upon the analytical framework that already exists for unfair contract terms, that is, whether there is a legitimate business purpose associated with the particular practice and whether it results in an imbalanced outcome for the consumer.

Marketing: addressing manipulation

Marketing that impacts or restricts the freedom of choice of a consumer (without good reason) might be considered manipulation and an unfair trade practice. Manipulation also involves consumer harm that is not reasonably avoidable by a consumer.

The widespread digitisation of commerce has given firms an enhanced ability, not only to compile detailed customer profiles, but also exploit consumers' cognitive biases and individual vulnerabilities. The collection of a greater amount of intimate and personalised data creates the opportunity to target market, and even subvert or manipulate reasonable decision-making by consumers.

A provision that enables consideration of the impact on the consumer (i.e. was, or is it likely, that harm is incurred) will improve the operation of consumer law; compared to unconscionable conduct which focuses on the conduct of the firm and whether it is against some sort of social norm.

Core product purpose: design and pricing

Clearly identifying a core product purpose is an important aspect of fairness, as it provides a yardstick for assessing consumer outcomes. A consumer product or service needs to have a reason for existing (other than a customer paying for and using it, and the firm supplying it).

A related aspect of fairness involves ensuring that the commercial returns to the firm associated with the product arise predominantly from consumer outcomes that are consistent with the product's purpose. This analysis would then help identify unfair practices—such as, offering discounts to new customers that aren't replicated for loyal/ongoing customers (a problem in

insurance, mortgages, energy) or paying intermediaries (brokers, advertisers, comparison websites) rebates or commissions, creating risks associated with misaligned incentives.

This analysis builds on existing rules around fitness for purpose but has a greater focus on fair outcomes, that is, is the product or service likely to meet a consumer need. A key limitation of the existing ACL provisions relating to fitness for purpose is that they generally only apply if the consumer discloses their purpose for purchasing a particular product or service.⁴³ In most instances, consumers do not disclose a specific purpose.

Addressing vulnerability: universal design

Fairness is also about ensuring consumers experiencing vulnerability do not experience worse outcomes than more savvy consumers. Where consumers have limited ability to maximise their wellbeing, or have difficulty in obtaining or assimilating information, due for example to age, disability or background, they are less able to buy, choose, or access suitable products.

A requirement around fairness can require a better balance between business and customer responsibilities—it can help address the incessant problems caused by long and impenetrable terms and conditions by ensuring that businesses are more upfront with their customers. It can also require businesses to identify potential consumer harm caused by their products and service systems, adopting a ‘prevention is better than cure’ approach. Importantly, it can also address problems in the area of customer service and complaints processes, which can commonly benefit only those who are able to navigate the complexity rather than those who experience vulnerability. An unfair trade practice may be one that incorporates unnecessary barriers to service assistance.

Fairness can also help establish a universal approach to addressing vulnerability, moving away from a policy approach that focused solely on specific areas of disadvantage. In this way, a regulatory focus on fairness would improve the position of all consumers, including those who need more support due to their vulnerable characteristics or circumstances.

Recommendations

7. The Committee should endorse the development of an economy-wide prohibition on unfair trading practices, capturing FinTech practices.
-

⁴³ Sections 55 and 61, ACL.

Regulate Buy Now, Pay Later services

The Inquiry should scrutinise products such as Buy Now, Pay Later (BNPL) that market traditional financial products in different ways (such as through mobile apps) and claim it is “innovative” and good.

The explosion of BNPL services such as Afterpay and Zip come at a time when Australians hold record levels of household debt. As the popularity of these products have grown, so too have the numbers of individuals with debts owed to BNPL providers presenting to financial counsellors for assistance.

BNPL providers extend credit to individuals and profit through a mix of merchant fees, missed payment fees and other fees such as fixed upfront or periodic charges. By not charging interest on their loans, BNPL providers are able to skirt the National Credit Act and accompanying consumer protections. Categorising these companies as “innovative” because of slick marketing and their ability to evade responsible lending laws and lend through an app is ridiculous. ASIC’s Review of buy now pay later arrangements report noted a number of risks with this industry including:

- Pushing users into debt - one in six users had either become overdrawn, delayed bill payments or borrowed additional money because of a buy now pay later arrangement. Concerningly, 23% were making repayments with a credit card.
- Encouraging people to overspend – 81% of people believed that these arrangements allow them to buy more expensive items than they would otherwise and 64% of users were spending more than they normally would.
- Providers using behavioural techniques to influence consumers to make a purchase without careful consideration of the costs.⁴⁴

Innovation can produce significant benefits for consumers. However, not every product innovation is necessarily in consumers’ best interests. This is particularly the case in complex markets such as financial services, where the risks of bad product design and mis-selling can have catastrophic consequences. For example, we have recently seen “innovation” from payday lenders which has led to more online targeting and quick loan applications for high-cost debt.⁴⁵ We need to ensure that innovation leads to services that genuinely meet the needs of Australian consumers rather than exploit regulatory gaps and sell debt in a more effective way.

⁴⁴ Australian Securities and Investments Commission, *REPORT 600: Review of buy now pay later arrangements*, November 2018, available at <https://download.asic.gov.au/media/4957540/rep600-published-07-dec-2018.pdf>

⁴⁵ Dr Vivien Chen, *Payday Lenders: Trusted friends or debt traps?*, 15 October 2019, <https://www2.monash.edu/impact/articles/banking/payday-lenders-trusted-friends-or-debt-traps/>

Current approach to Buy Now Pay Later services

Buy Now Pay Later services are not specifically regulated as they do not fall within the auspices of the *National Consumer Credit Protection Act 2009*. This means that there are no requirements for:

- responsible lending checks
- internal dispute resolution
- external dispute resolution
- access to financial hardship arrangements

Many 'buy now pay later' providers have placed self-imposed limits on how much a consumer can spend, but these are purely voluntary and there is likely to be shareholder pressure to increase these limits. There is therefore no guarantee that these self-imposed rules will remain, or other services will provide limits at all.

As buy now, pay later services grow, pressure is likely to grow and spending limits will likely increase. Further, there is every possibility that other start-ups will step in and have much higher spending limits. Both of these eventualities will significantly increase debts incurred by consumers.

Reforms to address the harms caused by unlicensed financial service providers

At a minimum, the *National Consumer Credit Protection Act 2009* must be expanded to ensure that all buy now pay later services are required to be licensed and are subject to the same requirements as all other credit providers. Currently to get the *National Consumer Credit Protection Act 2009* to apply it needs to be proved that the cost is more than the cash value of the goods. This is increasingly difficult to achieve with goods, that are own brand or not easily comparable. Consumers are not willing to take the risk to test the matter in Court, and many buy now, pay later providers resolve the issues before it can be tested when the issues are raised

In addition to this the law to be expanded to address a number of the unique aspects of these services including:

- regulating late fees;
- limiting multiple accounts;
- ensuring appropriate identity checks;
- ensuring users who have been blocked from further borrowing can still access their accounts for the purposes of monitoring their debt, repayments and the application of any fees and charges; and
- restricting the use of these services by minors.

Recommendations

8. Expand the *National Consumer Credit Protection Act 2009* to ensure that all buy now pay later services are required to be licensed and are subject to the same requirements as all other credit providers including internal dispute resolution and membership of AFCA.
9. Future-proof reforms to *National Consumer Credit Protection Act 2009* to capture new products and services, and prevent harmful practices from emerging and enact a broad and robust anti-avoidance provision.
10. In addition to this the law to be expanded to address a number of the unique aspects of these services including:
 - a) regulating late fees;
 - b) limiting multiple accounts;
 - c) ensuring appropriate identity checks;
 - d) ensuring users who have been blocked from further borrowing can still access their accounts for the purposes of monitoring their debt, repayments and the application of any fees and charges; and
 - e) restricting the use of these services by minors.
11.

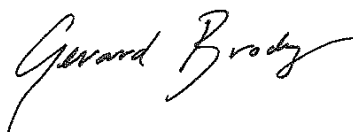
Concluding Remarks

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 at Financial Rights on (02) 8204 1386 or at drew.macrae@financialrights.org.au.

Kind Regards,



Karen Cox
Chief Executive Officer
Financial Rights Legal Centre



Gerard Brody
Chief Executive Officer

