Financial Rights
LEGAL CENTRE

12 September 2019

Digital Platforms Inquiry
Structural Reform Division
The Treasury
by email: DPIConsultation@treasury.gov.au

## Digital Platforms Inquiry

Thank you for the opportunity to comment on the final report of the ACCC Digital Platforms Inquiry. This is a critically important roadmap to promote much needed change. The Financial Rights Legal Centre (**Financial Rights**) will address the recommendations arising out of Chapter 7 with respect to Digital platforms and consumers. Our interest in the Digital Platform Inquiry is centred on the need for a strengthened privacy regime arising out of increasingly common data use and collection practices as identified in the Final Report and their impact upon financial services consumers and in particular those experiencing some form of vulnerability.

Financial Rights has worked extensively on the impact on consumers of the digital economy – particularly in the financial services sector. The views in this submission are drawn from multiple submissions and consultations on the introduction of Open Banking, the Consumer Data Rights, Credit Reporting, the use of Artificial Intelligence.[1]

We strongly support recommendations 16 through to 21 as critical regulatory infrastructure for a modern digital based economy - infrastructure that places the consumer interest at the heart of the digital bargain and baking in consumer protections to prevent harm and exploitation, increase transparency, and empower consumers.

The recommendations need to be implemented in full to ensure that Australian consumers do not end up lagging behind the rest of the world but also to ensure Australian based businesses do not end up fundamentally disadvantaged in the international digital marketplace.

## Recommendation 16: Strengthen protections in the Privacy Act

Financial Rights supports strengthening the protections in the current *Privacy Act* with the introduction of key amendments to:

- update the "personal information" definition;

[1] https://financialrights.org.au/submission/

- strengthen notification requirements;
- strengthen consent requirements and pro-consumer defaults;
- enable the erasure of personal information,
- introduce direct rights of action for individuals and
- increase penalties for breaches.

We wish to make specific comments regarding three of these proposed amendments: notification, consent and erasure. While acknowledging the limits of disclosure and placing the onus on consumers to assert their rights against unsafe and harmful digital products and services,[2] these three protections are critical pieces of infrastructure for empowering consumers to exercise greater choice and control over their engagement with digital platforms across the economy. Each has been implemented in Europe raising levels of consumer protection and accepted, implemented and promoted by digital platforms in that jurisdiction. Without these protections both Australian consumers and Australian businesses will fall behind in the digital economy, with the latter potentially being significant disadvantaged when competing in the international marketplace – which is where success in the digital economy lies.

**Strengthen notification requirements**

Financial Rights supports strengthening the current notification requirements under APP 5 to notify consumers of the collection of their data. It is currently left up to the APP entity to decide whether and how to provide notification under APP 5. This is unacceptable for a data-heavy economy.

Financial Rights supports the notification being:

- concise, transparent, intelligible and easily accessible, written in clear and plain language (particularly if addressed to a child), and provided free of charge; and
- consumer tested.

We also support APP 5 explicitly specifying the information that must be set out in the notification, including:

- the identity and contact details of the entity collecting data;
- the types of data collected and the purposes for which each type of data is collected; and
- whether the data will be disclosed to any third parties and, if so, which third parties and for what purposes.

We wish to note a couple of issues.

[2] As outlined in the submission of the Consumer Action Law Centre to this consultation, Financial RIgths supports reforming privacy law (including any codes regulating digital platforms) in a way that promotes greater use of consumer defaults, recognising the limitation of consent mechanisms https://consumeraction.org.au/wp-content/uploads/2019/09/190902-Consumer-Action-sub-Digital-Platforms-Final-Report.pdf,

The draft CDR legislation states that a participant "must take steps" rather than "must take reasonable steps." This is a simple solution to address the core problem.

Under the ACCC CDR Rules, notification must include "the data that has been requested."[3] The conception of data here is more specific than that proposed by Recommendation 8(a) which is the "types of data." "Types of data" has the potential to be much broader. Consideration needs to be had regarding the level of data description that is appropriate and what will be most comprehensible to a consumer. Once that is decided there needs to be consistency across the CDR and the *Privacy Act*.

Article 13 of the GDPR requires notification of:

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing[4]
- transfer personal data to a third country or international organisation[5]
- the period for which the personal data will be stored[6]
- the existence of the right to request from the controller access to and rectification or erasure of personal data[7]
- where the processing is based[8]
- the right to lodge a complaint[9]
- whether the provision of personal data is a statutory or contractual requirement[10]
- the existence of automated decision-making, including profiling[11]

All these should be included in any notification.

Financial Rights does not support an exemption to the proposed notification requirements, where personal information is collected for non-commercial purposes and in the public interest. Full transparency should be required in *all* cases. While non-commercial cases may entail less risk of commercial exploitation, the collection of consumer data still involves significant risks including hacking and use for activities that they may not feel comfortable with or with to be a part, eg political, religious or other campaigning uses. A consumer should have a comprehensive right to know what data is being collected and how it is potentially going to be used, handled and stored.

---

[3] Rule 9.3.2, ACCC Consumer Data Right Rules Framework, September 2018,

[4] Article 13(1)(c)

[5] Article 13(1)(f)

[6] Article 13(2)(a)

[7] Article 13(2)(b)

[8] Article 13(2)(c)

[9] Article 13(2)(d)

[10] Article 13(2)(e)

[11] Article 13(2)(f)

Finally it is important to note that while notification is important it is not the sole solution to the problem and nor should it be relied upon to solve the problems raised by the ACCC report.

Mere disclosure is a limited and inadequate tool for addressing problems for consumers in the financial services sector and other areas of the economy. Financial Rights agrees with CHOICE when it states in its submission that:

> *Rather than forcing a consumer to understand how a product may be harmful for them, it is far preferable to hold the company to account for providing that harmful product. This holds true for digital platforms as much as it does for other industries.*

The measures to be taken should keep this mind and shift the onus away from consumers and raising their literacy back on to digital platforms and other providers to develop safer, more appropriate products and services in the marketplace.

**Strengthen consent requirements and pro-consumer defaults;**

Financial Rights supports amending the *Privacy Act* to define 'consent' to include only *express* consent and that the current non-binding elements of the OAIC's guidance regarding consent be binding requirements under the APPs, to ensure that:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

The EU has finalised guidelines on consent.[12] These guidelines should provide the government with significant guidance as to the nature of consent including examining a multitude of situations and concepts to enable genuine consent to be effective.

The *Privacy Act* was drafted during a period where the use of digital terms and conditions that are bundled and lengthy were relatively new. Their use has led to a significant asymmetry of information and power, working against the interests of consumers. They are unfair and have led to lower levels of product, service and data literacy.

The APPs (including APP3, 7 and 8) must be modernised and future-proofed with clear requirements on all companies (not just digital platforms and financial services) to gain express, fully informed consent from a consumer.

With respect to the specific elements that are currently included in the Consumer Data Rights Financial Rights makes the following observations and recommendations.

*Adequately informed:* It is important to ensure that the lack of consent for a particular use should not limit the ability to receive a service unless the data is fundamentally necessary for a particular product or service to work.

[12] The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data, Article 29 Working Party Guidelines on consent under Regulation 2016/679 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

*Voluntariness:* The EU guidance acknowledges that there are a number of situations where genuine consent cannot be freely given – for example in situations where there is a significant imbalance of power. This needs to be incorporated into any notion of voluntariness. To this end consent must be freely given, absent of any element of inappropriate pressure or influence upon the consumer preventing them from exercising their free will including:

- any imbalance of power;
- the presence of any conditions via for example, the bundling of consent of necessary and unnecessary uses;
- the conflation of several purposes without consent for each specific use; and/or
- detriment to the consumer if consent is withdrawn or refused;

*Current and specific consent:* Consent should also be able to be constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data. Entities must be obliged to only collect the minimum amount of personal information that the business actually needs. This means not collecting extra information simply for marketing purposes at some later date for example. Consent must also be time limited and should not be ongoing in perpetuity. Like the CDR rules there must a period of time where consent must be renewed.

*Understanding and communicating consent:* APP entities must explain in simple, clear, terms *why* information is being collected and for what it is being used.

As with notification and disclosure generally, Financial Rights does acknowledge that consent cannot be solely relied upon as a solution. Consent fatigue may arise as it already does with the current set of consents. This does not however mean that it should not be pursued. It does however again mean that the onus should be placed upon digital platforms to both ensure that consent regime is effective and engaging and that they meet higher standards to ensure that consumers are not harmed by a product if consent fails to be an effective tool for empowering consumers.

***Consent and minors***

Children are particularly vulnerable to the allure of new technology and new apps and may not fully understand the consequences of any consents required nor the full range of contractual obligations. The current consent regime does little to account for children's use of digital technology and must be addressed urgently.

We note that the EU's GDPR restricts the ability to consent to those 16 years (or potentially 13 years and above) depending on the State. Article 8 states:

> *Art. 8 GDPR Conditions applicable to child's consent in relation to information society services*
>
> 1. *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

2. *The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*

Minors are particularly vulnerable to exploitation and the risks versus potential benefits are high. For example, the Dollarmites program run by Commonwealth Bank in schools received a SHONKY Award in 2018 from CHOICE. The Dollarmites program works by offering commissions to primary schools in exchange for running the school banking scheme. The commissions include a one-off payment of $200 when the first student makes their initial deposit as well as annual rewards of up to $600 per year.[13] Recent investigations from Fairfax found that Commonwealth Bank staff fraudulently activated Dollarmite accounts for personal gain.[14]

We cannot see what would stop a bank, FinTech, digital platform or any other business from instigating similar marketing programs directed at children in the digital economy.

Just this week YouTube has been fined $170m by the US Federal Trade Commission (FTC) and New York State to settle allegations it collected children's personal data without their parents' consent. They found that the children's version of YouTube tracked information about what kids are watching in order to recommend videos and collected personally identifying device information.

The misuse of children's data and a lack of consent is particularly a concern in the FinTech sector since technologies provide the ability for individual consumers to retreat into private, hidden, digital spaces to transact with FinTech providers. Given the ease, speed and inherently private nature of using these technologies, the usual social cues and hurdles that would work to potentially stop someone from accessing harmful or unsafe digital products and services are simply no longer there. These issues are a problem for adults but the situation is exacerbated when we consider the use of phones by minors and a willingness to hide activities from guardians and parents.[15]

Digital platforms should be required to demonstrate that they have verified someone's age and identity before acquiring consent to share and or CDR data.

We note that the Final Report bundles children's consent into the proposed OAIC privacy Code for digital platforms. We not think that this issue should solely be addressed in the Digital Platforms Code alone and should be dealt with in the APPs.

**Enable the erasure of personal information**

Financial Rights supports the amendment of the *Privacy Act* to enable the erasure of personal information. Erasure should occur without undue delay as per Article 17 of the GDPR.

---

[13] https://www.commbank.com.au/personal/kids/school-banking/information-for-schools.html?ei=bld2-btn-information-for-schools

[14] https://www.smh.com.au/business/banking-and-finance/dollarmites-bites-the-scandal-behind-the-commonwealth-bank-s-junior-savings-program-20180517-p4zfyr.html

[15] Just as one example, Madhumita Murgia The secret lives of children and their phones, October 6, 2017 https://www.ft.com/content/7c972e2e-a88f-11e7-ab55-27219df83c97

We note that the ACCC supports the exception to erasure being

> *unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.*

We support the ACCC's position as it is important that these reasons align with public interest reasons not commercial or other self-interested business reasons. We think the proposed exception is broad enough to ensure that genuine and legitimate interests in retention are captured – in line with the GPDR which lists the following exceptions:

- exercising the right of freedom of expression and information: Article 17(3)(a)
- for compliance with a legal obligation, e.g. bank keeping data for seven years: Article 17(3)(b)
- for reasons of public interest in the area of public health: Article 17(3)(c)
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes: Article 17(3)(d)
- for the establishment, exercise or defence of legal claims: Article 17(3)(e)

The following elements from Article 17 should also be included to ensure erasure where:

- the individual objects to the processing of data – including direct marketing purposes and profiling: Article 17(1)(c) & Article 21
- the data was unlawfully processed: Article 17(1)(d)
- there is a legal requirement for the data to be erased: Article 17(1)(e)
- the consumer is a child at the time of collection: Article 17(1)(e) & Article 8

Consumers have the reasonable expectation that once a consumer withdraws consent or their consent is expired, that their information will be deleted or destroyed in order to protect their privacy.

Consumers do not want the situation where their data has been used by a company – with or without consent – and that company holds on to that data to use for secondary purposes, either in aggregated or de-identified form where there is any possibility of re-identification.

This expectation is also increasing as consumers become more and more aware of and literate regarding the extent their own personal data is being used and misused by companies, as outlined in the Preliminary Report.

Consumers should remain highly cynical of any regime that allows APP entities to hold on to their data after they leave a service.

Financial Rights continues to support automatic deletion after a set period of time in line with standards set by GDPR Article 17(1)(b) where the:

> *the relevant storage period has expired and the data holder doesn't need to legally keep it (such as banking records for a seven year time period).*

We note that the ACCC has recommended this obligation be set out in the Digital Platforms Privacy Code of Practice. This however will only apply to those entities covered by or

signatories to a DP Privacy Code. Similar automated deletion and retention periods will need to be applied to every other sector across the economy. This could be done so in piecemeal by the Consumer Data Right. However we believe that it is more appropriate to apply this right to all holders of data as a part of the Australian Privacy Principles and the Privacy Act.

### Recommendation 17: Broader reform of Australian privacy law

Financial Rights supports broader reform of Australian privacy regime to shift the perspective of Privacy laws away from creating an easier environment for digital platforms to retain, use and exploit private information and to one that more effectively support the interests of consumers by placing their interest front and centre of the regime.

To date this has not been the experience of Financial Rights as outlined in our earlier submission to the Digital Platforms Inquiry.

The reforms proposed regarding objectives, scope, standards of protections, de-identified information, overseas data flows and third-party certification would all help shift this emphasis and place a greater onus on APP entities and digital platforms to protect the interests of their customers, and produce safer, less harmful products, services, terms and conditions in the first place.

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

### Recommendation 18: OAIC privacy code for digital platforms

Financial Rights in principle supports the development of effective and enforceable Codes of Practice to improve consumer outcomes in areas where legislation fails to provide specific details. They are also, generally speaking, more easily reviewable and updated, in a dynamic industry – more so than changing legislation.

Financial Rights notes that the proposal has similarities to the current OAIC administered *Privacy (Credit Reporting) Code 2014*.

It is important that a Code of Practice for digital platforms be monitored by an independent administrative body.

The current governance structure for the Credit Reporting Code is not sufficiently robust to enable stakeholders to have confidence in the credit reporting system. Nor does it sufficiently deal with conflicts of interest.

Consequently, the establishment of an OAIC Code of Practice for digital platforms should be monitored by an independent Code Compliance Committee, established under the Code. This Committee should:

- be independent of the digital platforms sector (with a balance of industry representatives, consumer representatives, and an independent chair); and
- be provided with adequate resources to fulfil the relevant functions and to ensure that code objectives are not compromised

The current governance structure of the Credit Reporting Code relies almost entirely on Credit Reporting Bureaus monitoring Credit Providers' compliance with their Part IIIA obligations, incorporated in their agreements with the Credit Reporting Bureaus. This structure presents an unacceptable conflict of interest.[16] A similar mistake should not be made in an OAIC Code of Practice for digital platforms.

Financial Rights points to the Codes of Practice in Banking and Insurance as examples of ways to structure oversight.

Finally the Code of Practice provides an opportunity to address many of the issues raised in the Preliminary Report namely:

- the inconsistency and vague terminology used in privacy terms and conditions
- the difficulty in navigating terms and conditions
- the difficulties in accessing and finding privacy statements on websites;
- the use of vague and ambiguous language;
- the use of online tracking technologies;
- the difficulties in switching off location tracking

Other commitments can also be included in the Code of Practice including adhering to 'Privacy by Design' Principles, implementation of ethical data management principles and human design standards.

Finally Financial Rights wishes to reiterate CHOICE's view with respect to the need for appropriate representation in the development of a Code of Practice. CHOICE states in their submission

> *In an industry, you are likely to find multiple companies and peak bodies with the same or significantly overlapping interests. In contrast, there may only be a very limited number of organisations that can represent the needs of consumers in an unbiased way. When the seats at the consultation table are held by multiple industry representatives and a much smaller number of consumer advocates, the potential for the development of a code to be distorted so that it favours business interests is high. In short, codes that are led by industry tend towards favouring industry. CHOICE recommends that the OAIC or any other body leading this code development process keep this in mind, and consider ways of ensuring that representation among stakeholders is balanced.*

We agree with this and believe appropriate consumer representation should be included in the development of this Code of Practice.

## Recommendation 19: Statutory tort for serious invasions of privacy

[16] CPs are the paying clients of CRBs, and CRBs will necessarily be dis-incentivised to report their incidents of non-compliance under the Code. Even if each CRB establishes a documented, risk based program to monitor CPs' compliance, there will inevitably be less thorough reporting of all non-compliant activity than there would be under an independent administrative body. Less thorough reporting means that systemic problems will either not be identified or will continue for longer.

Financial Rights supports the ACCC's recommendation to introduce a statutory tort for serious invasions of privacy. This recommendation has been around since the ALRC examination of the issue and its implementation is long overdue to bring Australia into line with other jurisdictions.

This will be a positive step in the financial services sector as it increasingly moves into business models that are based on the use of new data collection technologies and data analytics in FinTech[17] and InsurTech[18]. 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, etc. FinTechs 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 also 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 get to know their customer more.

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. However the development of an increasingly accurate financial identity built by data has serious consequences and harms for consumers. A person's financial circumstance is highly sensitive since its use by financial institutions, or in other cases a breach causing a leak of this private information, opens them up to a range of significant problems.

A statutory tort will motivate current and emerging business models to not engage in harmful data collection and use practices and pay more regard to the consequences of the use and any potential breach of personal information.

**Non-digital serious invasions of privacy**

However it should also be noted that the introduction of a statutory tort for serious invasions of privacy should be designed and implemented not solely with digital platforms in mind. There are current non-digital practices by financial services companies that would and should be captured by a statutory tort for serious invasions of privacy.

---

[17] E.g. mobile and online banking; Open Banking; new personal financial management services; investment and wealth management services with automated or robo-advisers services; new lending and unsecured credit services based on data led credit-scoring and risk profiling; new payment services; encrypted digital wallets that stored bank, debit or credit card detailing for online payments; neo banks and FinTech savings banks; offline mobile payments; and credit scoring and social scoring

[18] Where 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 being put to specific use by the insurance sector. 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.

In insurance claims handling, assessment and investigation practices have a significant impact upon consumers – issues with investigation tactics and surveillance are one of the key issues complained about to the Insurance Law Service.

Without a statutory action for invasion of privacy any person can without your consent take photographs, still pictures and videography of you in a public place. In addition, any information that is publically available can be sourced. Insurers also will sometimes allow themselves the right to undertake surveillance of their insured's in the contract of insurance. This contractual right does not extend to non-parties to the insurance. But, as stated, there is no restriction on the practice of still photography, and filming or monitoring of third parties in public places, places of work and businesses.

Surveillance device laws theoretically provide a level of protection against the unwarranted, intrusive or inappropriate surveillance of Australians, including insurance claimants. While laws are in place in each state and territory to regulate the use of surveillance devices, their complexity, inconsistency and failure to keep up with technological progress provide irregular protection and little comfort to parties subject to intrusive and unwarranted surveillance. See further information in the Financial Rights' Report *Guilty Until Proven Innocent: Insurance Investigations* in Australia.[19] In the end though while much of the surveillance undertaken by life insurance investigators is legal, the conduct of the surveillance does veer into ethically murky territory.

We note that the ALRC considered the need for a specific defence to protect investigations into potential fraud or misrepresentation

It stated that:

> *It is in the interests of all policy holders that insurers have safeguards against fraudulent claims. Where they have reasonable grounds for suspecting fraudulent conduct, they or others on their behalf may often carry out investigations that could be viewed as invasions of privacy. The defence that the conduct was required or authorised by law is wide enough to cover these circumstances. … The ALRC considers that individuals or organisations that engage in such conduct may be protected from liability under the public interest balancing test.*

Financial Rights supports the reasons but believes that insurers have not acted in ways that either demonstrated reasonable grounds for suspecting fraudulent conductor acted in ways that met expectations of privacy.

ASIC's recent report into car insurance investigations found that:

> *Fraud is a real and serious issue and insurers need to investigate, identify and deny fraudulent claims. But our data shows that of all the claims that insurers decided to investigate, only 4% were declined for fraud, and only 10% were declined for some other reason. Over 70% of the claims that insurers investigated were paid.*

This clearly demonstrates that while there is a public interest in preventing fraud the grounds upon which insurers are undertaking investigations (that can involve serious invasions of privacy) are not as robust or as reasonable as they claim.

---

[19] https://financialrights.org.au/wp-content/uploads/2016/03/Guilty-until-proven-innocent.pdf

> *Consumers expect a fair process to be followed when a claim is investigated. Consumers in our research whose claims were investigated and eventually paid felt angry, frustrated, confused, overwhelmed and helpless during investigations*

In developing the statutory tort, it is critical that it is designed in a way to ensure that defences are not used as carte blanche get-out-of-gaol-card-free cards to act in unreasonable ways that invade people's privacy.

## Recommendation 20: Prohibition against unfair contract terms

Financial Rights supports amending the Competition and Consumer Act 2010 to ensure that unfair contract terms are prohibited and not just voidable, with civil penalties applying.

Currently without civil penalties financial firms are able to include unfair terms that serve their interests, with individual consumers and their representatives forced to identifying these terms and argued for them to be declared void. This is incredibly difficult in an environment with long, overly complex terms and conditions. This also has very little impact on a firm where there is no money exchanged in the digital economy.

## Recommendation 21: Prohibition on certain unfair trading practices

Financial Rights supports a prohibition on unfair trading practices. Financial Rights accepts that the prohibition should be targeted and defined for the purposes of certainty but that it should it should be designed to capture harmful practices that disproportionately impact negatively upon people experiencing financial vulnerability including price discrimination, risk segmentation, profiling for profit, predatory marketing and the delivery of poor, unsuitable products. For example, those experiencing financial hardship are often very profitable to debt management firms and fringe financial service providers and therefore most vulnerable to exploitation. Those in more precarious financial situations are more likely to be unfairly charged higher amounts or pushed to second tier and high cost fringe lenders.

We would also recommend that the prohibition be designed to address issues arising out of the use of closed proprietary algorithms. These can lead to situations where consumers are denied access to crucial products and services based on inaccurate data without the ability to determine why or to correct underlying assumptions. Increased use of non-transparent, black box technology could also lead to poor consumer outcomes through the creation of potentially biased and discriminatory algorithms.

We have had the opportunity to read Consumer Action Law Centre's submission to the Review and endorse their position with respect to unfair trading practices and recommendations 1 and 2:[20]

[20] Page11, Consumer Action Submission re: Final Report of ACCC Digital Platforms Inquiry https://consumeraction.org.au/wp-content/uploads/2019/09/190902-Consumer-Action-sub-Digital-Platforms-Final-Report.pdf

*Recommendation 1 Address unfair trade practices through a simple, principles-based, outcomes-focused new provision in the Australian Consumer Law prohibiting unfair trade practices, including practices that are likely to have an unfair outcome.*

*Recommendation 2. The scope of the provision should not be limited, but regulatory guidance can be provided to help businesses understand what is meant by unfair conduct or practices, including in the areas of:*

- *Marketing and sales, particularly addressing harm associated with consumer manipulation;*
- *Product or service design and pricing, drawing on the concepts of a legitimate business purpose and fitness for purpose; and*
- *Customer service and complaints processes, ensuring service is responsive to customer vulnerability.*

## Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights on (02) 9212 4216.

Kind Regards,

Karen Cox
Chief Executive Officer
Financial Rights Legal Centre
Direct: (02) 8204 1340
E-mail: karen.cox@financialrights.org.au

## About Financial Rights

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