24 December 2020

Secretariat
Payments System Review
The Treasury
Langton Crescent
PARKES ACT 2600
PaymentsReview@treasury.gov.au

Payment System Review – Issues Paper

Thank you for the opportunity to comment on the Payment System Review.

The Financial Rights Legal Centre (**Financial Rights**) will address the questions and issues raised in the paper from the perspective of the payment system problems faced by consumers we speak to in our practice on the National Debt Helpline and Mob Strong Debt Help line.

The problems we see range from the inability to quickly and efficiently resolve issues when things go wrong with the current regulated payment system, to the impact on consumers of new payment systems. Many of the systemic issues faced by consumers are fundamentally borne of form of regulatory oversight in place, the lack of oversight or the gaps in the complex regulatory regime. In so identifying these, this submission largely aims to answer questions 3 and 4:

- Question 3: What is the appropriate balance between self-regulation, formal regulation and government policy to ensure the payment system continues to work in the best interests of end-users?
- Question 4: Are there gaps (or duplication) in the current architecture that need addressing to ensure the system continues to work in the best interests of end-users?

In so doing we aim to ground a consideration of the regulatory framework in the practical everyday lived experience of consumers who are at the receiving end of poorly constructed/conceived regulatory frameworks.

Some of the issues raised in this submission could be resolved within the current frameworks. However we would posit that - given the ongoing nature of many of the problems and their lack of effective redress, - the issue may lie with the effectiveness of the regulatory framework itself – including in particular the flaws of co-regulation and self-regulation.

This submission focuses on:

- the voluntary ePayments Code and the significant gaps and flaws of this Code and its impact on consumers;
- the difficulties of cancelling direct debits and recurring payments including the failure of self-regulation to resolve the issues
- the lack of regulatory oversight of Buy Now Pay Later services and
- the impact of Open Banking and the Consumer Data Right.

The ePayments Code

The most common way consumers actively engage with payment systems regulation is not when things go smoothly but when things go wrong. And the key regulatory tool (outside of financial services and consumer credit licensing and the *National Consumer Credit Protection Act 2009)* to assist consumers when things go wrong is the ASIC administered, voluntary ePayments Code.

The Code seeks to commit industry to require subscribers to the code to:

- give consumers terms and conditions, information about changes to terms and conditions (such as fee increases), receipts and statements
- set out the rules for determining who pays for unauthorised transactions, and
- establish a regime for recovering mistaken internet payments

However the ePayments Code is flawed.

The fact that the ePayments Code remains voluntary remains a significant gap in consumer rights and a failure of the payments system.

It is now more than a decade since ASIC first raised the issue of whether the Code should be made mandatory.[1] Subsequently, the Financial Services inquiry[2], published in 2014, recommended that the ePayments Code should be mandatory. The following year the then Government responded[3]:

> '*We will ensure that minimum acceptable practices consistently apply to the payments industry in the interests of consumers. ASIC will mandate baseline consumer protections in the ePayments Code, subject to the code being fit for purpose and technologically neutral.*'

We note too that the recent Hayne Royal Commission recommended financial services industry codes of practice be made mandatory and enforceable. The e-Payments code should be treated similarly to ensure greater compliance.

[1] https://download.asic.gov.au/media/1329878/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf

[2] http://fsi.gov.au/publications/final-report/

[3] https://treasury.gov.au/sites/default/files/2019-03/Government_response_to_FSI_2015.pdf

We are disappointed that creating a more robust ePayments regime has not been a priority. Consumers face real and ongoing harm because of this failure.

The objectives of the Code are set out in Chapter A of the code and can be summarised as follows:

- A quality consumer protection regime
- A framework to promote consumer confidence
- Effective disclosure to enable informed choice by consumers
- Clear and fair rules for allocating liability for unauthorised transactions
- Effective complaints procedures
- A flexible regime that accommodates providers of new services.

These objectives are generally very welcome from a consumer perspective – though there is a question whether they remain fit for purpose. It is, for example, worth considering whether the emphasis on 'effective disclosure to enable informed choice by consumers' reflects current insight and regulatory practice in relation to consumer behaviour and information remedies.[4]

Our overarching question, though, is whether these objectives are being met, or indeed could ever be, by the current regime. The regulatory model in which the Code sits, the Code's scope and drafting, and the application of the Code all appear to fall short of these objectives.

The ePayments Code should:

- should apply to all electronic payment systems;
- it should set out in simple terms consumers' rights and the obligations on regulated businesses;
- there should be effective monitoring of and reporting on both business practices and consumer experiences;
- there should be meaningful sanctions to create an effective deterrent for non-compliance, and
- it should be reviewed and updated regularly to take account of changes in technology, industry practices, consumer behaviour and the activities of third parties such as those perpetrating scams.

None of these are currently the case.

Our main concerns with the voluntary regime include:

- Although all major banks subscribe to the Code, the development of parallel schemes (such as for the New Payments Platform) has the potential to create consumer confusion, inconsistent standards and gaming by businesses.

[4] See: ASIC REP 632 Disclosure: Why it shouldn't be the default https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/

- Consumers might reasonably expect that the ePayments Code covers all ePayments, and this has in the past been ASIC's aspiration, but it does not now.
- The ePayments Code is applied by the Australian Financial Complaints Authority (AFCA) to its members, which gives it more bite than would otherwise be the case[5]. However, the inability of ASIC to enforce most provisions still lessens the impact of the ePayments Code.
- Furthermore not all relevant entities have to be members of AFCA, and there are monetary limits and compensation caps in place. While many voluntarily join AFCA the problem is that can withdraw their membership at any time.
- ASIC has no wider strategy in this area – the only reference to ePayments in the 2018-22 Corporate plan[6] is about making the Code mandatory – and it appears to have devoted very limited resources to ePayments work. This may be a product of its lack of enforcement powers, but even so we think there is scope for a more energetic and creative approach.
- The voluntary approach and absence of enforcement powers appears to have had an impact on the development of the Code itself. There seems to be a perceived need for ASIC to negotiate and compromise with businesses, with the result that softer protections are in place than would be the case in a standard regulatory regime. ASIC described[7] the previous Electronic Funds Transfer Code as being 'consensus-based' and said at the time of implementing the ePayments Code that 'Being voluntary, the Code needs to be sufficiently attractive to potential subscribers.' This is not a good basis for achieving effective customer protection and in turn a high level of consumer confidence.
- There is no transparent monitoring of compliance with the Code, no use made of research on the consumer experience, and no dedicated engagement on ePayment issues with consumer advocates.

There are two further specific issues relating to consumer engagement with the payment system and the flaws in the ePayments Code – its application to mistaken payments and unauthorised transactions. These are worth exploring in more detail to enliven any consideration of the regulatory structure, the end user's experience and the gaps.

The ePayments Code and mistaken payments

The ePayments Code covers mistaken payments, where the payment is sent to someone other than the intended recipient.

5

6 https://download.asic.gov.au/media/4855947/asic-corporate-plan-2018-22-focus-2018-19-published-31-august-2018.pdf

7 https://download.asic.gov.au/media/1343510/rep218.pdf

There are other types of mistaken payment, which the ePayments Code does not cover but in our view should. An error in the payment amount is not treated as a mistaken payment, for example.

Case study – Clara's story

A consumer told CHOICE:

'I have had the opposite problem of money by EFT into one of my accounts. Some might think this is not a problem, lucky?

The source was a betting company. I contacted my bank and nothing came of it. After more than 6 months it was several thousand dollars! I went to the bank again. Nothing more to do. Wow! I knew better?

More than a year later I found myself with a rather blunt letter asking, demanding I transfer the funds back to the bank! It was very disappointing that there was not a better way to manage this, especially when one tries to do the right thing and avoid a bigger problem. Was the bank really appreciative of my prior efforts and nice about it. Not in the slightest. In fact the banks initial approach was veiled and appeared similar to that a scammer might use.

Something is seriously wrong with the system if it cannot resolve such faults more promptly.'

Source: CHOICE community forum https://choice.community/t/have-you-had-problems-with-electronic-transactions/17529

Many consumer may believe they do not have to check the account numbers they input, in spite of any warnings to do so. This is because they may believe that if they enter the correct name, they will receive some kind of signal that the account number does not match.

It would appear that in such cases consumers assume that because banks' own systems connect account name and numbers, this will be built into the consumer interface of electronic payment systems too. This does not feel an unreasonable expectation, and at the very least the design of warnings to customers should take account of any such perceptions – though we agree with the concerns set out in the consultation paper about the likely ineffectiveness of risk warnings in general. The most effective approach is likely to be to bring the payment system in line with customer expectations. It would appear that the PayID service which uses the New Payments Platform may represent a step forward in this respect, though many more customers still use BSB and account numbers and so have a service that is more open to error.

We have seen many examples of blame shifting between banks: one bank says that it is the other bank that they are waiting on, and vice versa. The Code stipulates that it is the original bank's issue to address, but in practice this is not made clear to customers. Under the Code, a customer

should go to the sending ADI's EDR scheme, and both ADIs must cooperate with the sending ADI's EDR scheme.

At present, there is in reality often little or no recourse, particularly if the person that the money was accidentally sent to has already spent it or transferred it elsewhere. These can in theory become civil matters, but banks will usually not disclose the name of an account holder. This means that it can be difficult for consumers to even know who to initiate civil proceedings against, quite apart from the prohibitive cost of legal proceedings. This is one of the most common ePayments issues that we receive calls about.

The ePayments Code does not currently include any timeframes for banks dealing with mistaken payments – yet it is important to move quickly to get money back before it is spent or moved elsewhere. We consider that the ePayments Code should include timeframes for both the sending and receiving institution to act when notified of an issue.

The ePayments Code also is limited to online transactions only and does not require any of the principles to be applied to paper based errors.

Case study – Betty and Barney's story - C157391

Betty and Barney are retiree's in their 80's, they receive a small pension of $530 each month from a superannuation fund. They became aware after 6 months that they were not receiving the payments and contacted the superannuation fund attached to an authorised deposit taking institution. In completing the authorisation, they had made a small error on the form. The funds were correctly paid to the credit union, but not to their account. They instigated a trace on the funds. The credit union took 3 months to recall the funds and advised the account holder declined to return the funds. Betty and Barney raised a dispute under ePayments Code, by analogy citing the lack of warning on the form provided and the time frames of the entities in seeking the refund. Ultimately, they were provided a partial refund. The entities argued the ePayments Code did not apply. However, many of the protection principles equally applied including warning of mistakes in the form and the time frames to seek a refund. It was disappointing the entities did not take the approach of the ePayments Code which would have enabled Betty and Barney to recover all of their funds.

We put these concerns to ASIC in May 2019. They have yet to be addressed. We do however understand that ASIC plan to make some changes to the mistaken payment rules to put a greater onus on financial institutions, including allowing an AFCA complaint against a receiving institution. We also understand that they will make minor changes to warnings, but will not require double entry/name & account number matching as we have recommended. They claim this is difficult in practice and want to see ongoing engagement between industry and other stakeholders and industry solutions through NPP, PayID etc.

This means the problem is very likely to remain for the foreseeable future – despite this causing consumers' ongoing harm.

The ePayments Code and unauthorised transactions

The ePayments Code as currently drafted and interpreted does not adequately take account of the changing nature of scams and associated consumer behaviour..

We are particularly concerned about scams where the consumer is tricked into authorising a payment to an account that they believe belongs to a legitimate payee but is in fact controlled by a scammer.

In the absence of robust published data[8], it is hard to assess precisely the prevalence of such scams, but we understand they are very substantial and growing, and action is needed now to protect consumers. In 2016, this was the subject of a 'super-complaint' by our colleagues at Which? in the UK[9], which has subsequently led to the development of significant new rules that take effect on 28 May[10]. These ensure amongst other things that where neither the bank nor the customer was at fault, the customer should be reimbursed.

One issue to consider here concerns the meaning of 'unauthorised' and 'authorised', and (as set out in clause 11.8(a)) 'all reasonable explanations for the transaction occurring.' The nature of these scams is such that the consumer does literally authorise a transaction, but in doing so thinks that they are authorising a different transaction. In this respect it bears significant similarity to a mistaken payment. Indeed the Australian Payments Network describes[11] mistaken payments as including when the consumer 'had been given incorrect BSB or account details' – the difference being that in the case of scams the incorrect account details are supplied deliberately, not in error.

The current ePayments Code does explicitly mention fraud – but where this is due to someone working for a Code subscriber or a merchant, rather than for example someone purporting to work for a subscriber.

Case study – Clara's story

Clara voluntarily gave over her internet banking password to her partner for the purpose of him taking out an initial personal loan. The partner later became controlling, changed Clara's password to lock her out of her accounts, applied online for other debts without her knowledge, and changed her phone, address and email details with her bank. Clara was unaware of the additional debts as her account contact details had changed. She knew she did not have access to her accounts, but had no idea that further loans were being applied for.

[8] Card not present' fraud grew by 7.8%, to $478 million, in the year to 30 June 2018 https://www.auspaynet.com.au/insights/Media-Release/Steps-to-take-when-shopping-online-over-the-Christmas-period

[9] https://www.psr.org.uk/sites/default/files/media/PDF/which-super-complaint-sep-2016.pdf

[10] https://www.psr.org.uk/psr-publications/news-announcements/PSR-welcomes-industry-code-to-protect-against-app-scams

[11] https://auspaynet.com.au/resources/direct-entry/mistaken-payments

The proceeds of the first three personal loans were all paid into her account, then transferred to her online savings account, and then slowly spent. The transaction history therefore wouldn't have been indicative of fraud. However, there were four debts totaling $50,000 taken out with the same bank through internet banking over the period of seven months, to a 19-year-old customer. This potentially should have raised some red flags. Only the last credit card application raised red flags regarding verifying identify, however the card was still ultimately approved.

Under the ePayments Code as it stands, Clara is apparently liable for these debts as she initially gave out her password and did not report fraud or other issues to her bank. There are some protections in the Code relating to limiting losses to the transaction or daily limit on the account, but none of these apply in this case as these sections don't contemplate an entire loan application being the unauthorized transaction, even where the person was not in control of the application process or setting up of any limits to begin with.

The Ombudsman has made some determinations which provide greater protection to consumers who are the subject of scams where they have been tricked into sharing their details – see case study below. This is very welcome, but it is apparent that this interpretation is not being applied consistently by Code subscribers. It would be very helpful to have the Code state this position more clearly.

Case study – FOS decision about voluntary disclosure and extreme carelessness[12]

The customer received a text message which appeared to be from his bank, saying that his account had been locked and asking him to enter his log-in details. He did so. The message was in fact from a scammer, who then used his account to buy various goods amounting to more than $5000. The Ombudsman determined that entering his security details was not 'voluntary disclosure' as understood in the context of the ePayments Code. 'I consider that this provision of the Code was intended to deal with situations where a customer knowingly and voluntarily gave their details to another party with the understanding that they would be able to conduct a transaction (such as giving someone your PIN and Card to take money out of an ATM for you). The applicant thought he was unlocking his account with the FSP when he entered his account details into the link sent in the fraudulent text message. This was not "voluntary disclosure".'

[12] CFA summary of FOS case number 526294, 5 September 2018 https://service02.afca.org.au/CaseFiles/FOSSIC/526294.pdf as used in the Consumer Federation of Australia submission to the ASIC Review of the ePayments Code: https://download.asic.gov.au/media/5293715/cfa-cp310-submission.pdf

The Ombudsman also considered whether the applicant acted with extreme carelessness in failing to protect the security of his pass codes, and concluded that he had not, because:

- 'the applicant clicked on a link in a text message that appeared in a thread of messages that he had previously received from the FSP. It was therefore not unreasonable for the applicant to assume it was a legitimate text
- the FSP says that they warned all of their customers on account statements and on their website but this does not absolve them of all responsibility under the ePayments Code
- if a person is the victim of a sophisticated scam, such as this, and cannot reasonably viewed as being extremely careless, it will not be sufficient for the FSP to say they made their customers aware of scams
- there is nothing to indicate that the applicant had been made aware of the scam by having previously been a victim of it such that I would expect him to be more careful. For these reasons, I am not satisfied that the FSP has proven that the applicant contributed to his loss.'

Another form of unauthorised transaction relates to screen-scraping services and aggregators, which can require consumers to provide their passwords to a third party and so inadvertently breach the ePayments Code. Some of these practices are the product of other regulatory provisions. It is plainly unfair for consumers to lose protection in one area of regulation because of the application of regulation designed to protect them in another area.

Staff may be unaware of the ePayment Code's provisions or may seek to take advantage of consumers' lack of knowledge – see case study below.

Case study – Rosie's story

Rosie's transaction card was stolen from her house. She had written her PIN on the bottom of a face cream container in a different room to where she had left her card. $2,000 was withdrawn from her account using her card and the correct PIN. Her credit union refused to reimburse on the basis that she had written down her PIN.

The ePayments Code stipulates that a reasonable attempt to protect the security of a pass code includes hiding the code in a place that you would not expect to find it. Rosie was not aware of this protection in the Code, and her credit union either was also unaware or deliberately kept this from her.

Late last year the Australian Banking Association published its Accessibility Principles for Banking Services[13], which places emphasis on what it calls '*inclusive design*.' The Code is now out of line with this, for example in relation to protection of passwords, where a consumer might share their password with a family member or trusted friend to use services that they would otherwise be unable to access. This is considered in more detail in the ABA's Guiding Principles for Accessible Authentication[14]. It feels like there is a much more sophisticated understanding of consumer diversity, behaviour and needs in these documents than there is in the ePayments Code.

Case study – EFTPOS machine accessibility[15]

Legal action challenging the accessibility of the Commonwealth Bank of Australia's touch-screen 'Albert' EFTPOS machines for people who are blind or vision impaired settled last year. The CBA agreed to introduce a range of changes to ensure better accessibility of the Albert machines and committing to accessibility in future product development.

In settling the claim brought by Graeme Innes and Nadia Mattiazzo, who were represented by PIAC, the CBA acknowledged the difficulty Australians who are blind or vision impaired have experienced using Albert's touchscreen technology to enter their PINs.

There are other potentially adverse consequences for consumers of poor design by banks. For example, many ATMs now have a notice saying that the consumer should use their hand to screen the keypad when entering a PIN, so that the number cannot be filmed or otherwise observed. This may be hard for many people to do without them making more errors when using the keypad. But more generally it seems an inadequate fix for what appears a basic design failure, and may place an unreasonable burden on consumers. In such circumstances we would not expect the consumer to be liable for any unauthorised transactions that result from PINs being stolen when using an ATM.

As we understand it – ASIC's current position is that ASIC will not make changes to address scams via this code and that AusPayNet are doing things that may not be transparent to consumers.

[13] https://www.ausbanking.org.au/images/uploads/Accessibility_Principles_for_Banking_web.pdf

[14] https://www.ausbanking.org.au/Industry-Standards/guiding-principles-for-accessible-authentication

[15] CFA summary of https://www.piac.asn.au/2019/01/10/a-step-in-the-right-direction-cba-to-improve-accessibility-of-albert-eftpos-machines/ as used in the Consumer Federation of Australia submission to the ASIC Review of the ePayments Code: https://download.asic.gov.au/media/5293715/cfa-cp310-submission.pdf

They also planning to make some changes to pass code requirements to recognise customer vulnerability but the ePayments Code will not 'prohibit or expressly permit' screen scraping – a non-sensical position given it goes against all other Government and industry e-safety advice.

Both of these substantive examples – the ePayments treatment of mistaken payments and unauthorised transactions – and the lack of any substantive movement to address these serious consumer issues raises serious concerns about the effectiveness of the voluntary co-regulatory scheme. Consideration needs to be had over whether this is the best way to serve end user interests.

Cancelling direct debit payments and recurring payments

A significant gap for consumers relating to the functionality of the retail payments system that needs to be addressed is the lack of effective regulatory oversight of direct debits and recurring payments. We note that the RBA is looking at this issue in its Retail Payments Review where it is examining the:

> *capabilities around and management of automated and recurring payments, in particular arrangements for management of direct debits. End-users have periodically noted to the Bank that cancellation or redirection of direct debit and other automated payment arrangements is not always straightforward.*[16]

This issue is particularly frustrating for consumers and has been equally frustrating for consumer representatives for many years in seeking common sense changes to industry practice.

Firstly, consumers have long held significant concerns with the way banks deal with requests to cancel direct debits on eftpos cards. In our casework experience, subscribers routinely fail to comply with requests to cancel direct debits, instead regularly sending customers to the debit user. Interactions with the card issuer – Mastercard or Visa – also regularly result in being sent to the debit user.

The Customer Owned Banking Code Compliance Committee (COBCCC) for example recently undertook further research into whether COBA members are complying with Section 20 of the Code of Practice to act promptly to cancel a direct debit facility linked to your transaction account.[17] They found that:

> *although there has been some further improvement, non-compliance is still unacceptably high. Customer service representatives gave a compliant response to an enquiry in only 57% of calls. At the same time, institutions' online information needs improvement and was found to be readily accessible on just 38% of websites.*

---

[16] RBA Review of Retail Payments Regulation: Issues Paper, 12 https://rba.gov.au/payments-and-infrastructure/review-of-retail-payments-regulation/

[17] Compliance with direct debit cancellation obligations disappointing A follow-up own motion inquiry by the Customer Owned Banking Code Compliance Committee March 2019 http://www.cobccc.org.au/uploads/2019/03/COB-OMI-Direct-Debit-21March2019.pdf

Consumers are reliant on Australian Banking Association (**ABA**) member banks and COBA member banks to meet commitments under Codes of Practice which as the above demonstrates they are not meeting to satisfactory levels.

At least ABA and COBA banks have made moves to commit to improve direct debit cancellation practices. The same cannot be said of their commitment to improve the cancellation of recurring payments.

The difference between cancelling a direct debit and cancelling a card payment is, understandably, very confusing to consumers. More and more people are being encouraged to establish recurring payment arrangements using Mastercard or Visa facilities. The rollout of new security measure such as 'Tokenization' and Authentication also prevent new difficulties when trying to cancel recurring payment arrangements. We understand that even in circumstance where an individual is issued a new card, this may not result in payments being stopped.

Both the new ABA Code and current COBA Code are inadequate with respect to the obligations of subscribers to address customer requests to cancel recurring payments. Banks argue that they cannot cancel these recurrent payments and that customers should instead request a chargeback from the credit card company.

As we understand the matter – the issue is one that requires significant negotiations between banks and Visa and Mastercard, and decisions about where costs will be borne. Given this, and the fact that there is little incentive to resolve the issue – no movement has occurred in resolving this basic problem.

This lack of movement has significant impact upon consumers – particularly those facing financial hardship and experiencing other forms of vulnerability that make it difficult or impossible to shut down a recurring payment.

Regulators need to intervene to ensure that the same rules apply whether a customer has a direct debit using a BSB and account number, or a recurring payment using Mastercard or Visa numbers. Banks and card issuers should be obligated to respond to requests to cancel recurring payments and provide simple online functionality to resolve this problem.

One further problem with the cancellation of direct debits – one that has a huge impact upon the financially vulnerable is the practice of establishing multiple direct debits. Businesses authorise multiple direct debit authorities so when a consumer cancels one direct debit, the business moves on to use another authorisation in an effort to stymie the cancellation of direct debits by consumers. We are aware of some companies using up to eight authorisations.[18] The practice is particularly prevalent in the payday lending sector.

Again there is no regulatory oversight of this practice to prevent abuse.

[18] We note for example, that Cigno's Third Party Direct Debit Authority Request includes eight direct debit user ID's of Ezidebit Pty Ltd: https://cignoloans.com.au/third-party-direct-debit-agreement/

The lack of regulatory oversight of Buy Now Pay Later services

One significant gap to the system is the lack of effective oversight of the growing Buy Now Pay Later segment. The Issues Paper notes that "BNPL arrangements operate on top of or in conjunction with existing payment systems but can also be used at the point of sale. This has led to questions as to whether such arrangements constitute a payment system."

We note too that the RBA is currently examining some but not all of these issues in its Review of Retail Payments Regulation.

The explosion in growth of new payment options such as BNPL providers have altered the payments landscape for Australian consumers. However, BNPL providers are thriving in a regulatory black hole, and the inability for merchants to allow surcharging for this payment option is distorting the market. While BNPL tout their payments options as 'free' for consumers when payments are made on time, there is clearly a cost to using these services. This cost is ultimately borne by consumers through increased prices, as merchant payment fees are built into the overall price of goods and through payment of late fees and other charges. That model however might change with new or existing market participants conceivably introducing new fees in the future. This was the trajectory for credit cards which were also "free" when first introduced but many now charge annual fees.

Late fees are most likely to impact the people who can least afford to pay them - people who cannot pay on time. These fees are unregulated and can vary between providers and can increase financial hardship for some people.[19]

While using BNPL might indeed appear 'free' for consumers who can pay on time, the industry profits in other ways. Merchants offering BNPL as a payments option are charged a percentage for each sale paid for using a BNPL provider, and often a set fee per purchase. ASIC's review of BNPL arrangements noted that:

> *'For each buy now pay later arrangement in our review, merchants are charged a fee equal to a percentage of the amount of the purchase. Some providers also charge merchants a fixed fee for each arrangement.*
>
> *The size of these fees depends on factors such as the volume of buy now pay later arrangements used by the merchant, the risk profile of the merchants, and the types of goods and services offered by the merchant.*[20]

BNPL providers prevent merchants from passing on the costs of customers that use the service. These costs range from 3 to 6 per cent of an item's purchase price. These costs are being passed on to all consumers through higher prices.

---

[19] We note that the Australian Finance Industry Association has released a draft voluntary 'Buy Now, Pay Later Code' for consultation, which states that fees will be capped, but does not set a limit. While we haven't yet responded to AFIA's consultation, we do not consider this Code replaces proper regulation of BNPL finance.

[20] ASIC, *Report 600: Review of buy now pay later arrangements*, November 2018, https://download.asic.gov.au/media/4957540/rep600-published-07-dec-2018.pdf, 24

BNPL costs are very high when compared to merchant service fees for four-party scheme cards which range from 0.6 per cent for large merchants to 1.5 per cent for merchants with a turnover of less than $100,000.[21] This means that the regulatory framework is no longer driving effective competition in the payments system through, for example, sending price signals to customers about the true cost of using different types of payments.

Payments regulation should be guided by what is in the best interests of end users – customers that use Australian payment systems to buy their groceries at the supermarket, shop for goods online or pay for their morning coffee on the way to work. The *Payment Systems (Regulation) Act 1998 (Cth)* identifies a number of public interest factors the RBA is to have regard to the desirability of payment systems including being:

- financially safe for use by participants; and
- efficient; and
- competitive; and
- not (in its opinion) materially causing or contributing to increased risk to the financial system.[22]

We consider that permitting surcharging for BNPL payments is consistent with these factors, and would encourage a more efficient and competitive payments market. This should be the outcome of the RBA review of retail payments regulation. It would be a concern to consumer groups if this were not to be the case.

We support a simpler, fairer system that effectively regulates BNPL payment options, and includes strong enforcement mechanisms. Increased transparency through surcharging will help consumers to better navigate the complex system of payments currently on offer, choose the least expensive payment method, and stop all consumers from cross-subsidising more payment expensive options. Additionally, we believe that payments regulation needs to be future proofed to prevent regulatory arbitrage and emerging businesses from acting in ways that are not in the public interest.

It is our view that BNPL is not a financially safe payments option for many. By not charging interest on the credit extended to users, BNPL providers have avoided being captured by the *National Consumer Credit Protection Act 2009 (Cth)* and accompanying consumer protections. These protections include:

- responsible lending checks;
- caps on fees and charges;
- external dispute resolution including mandatory membership of the Australian Financial Complaints Authority; and

---

[21] RBA Review of Retail Payments Regulation: Issues Paper, 20 https://rba.gov.au/payments-and-infrastructure/review-of-retail-payments-regulation/

[22] *Payment Systems (Regulation) Act 1998* (Cth) s 8

- access to financial hardship arrangements.

Compliance with these requirements under the *National Credit Act* promotes good customer outcomes and is in the public interest, particularly in the context of ballooning household debt. As it stands, when a customer opts to pay for a purchase using BNPL, they are denied a raft of rights and protections compared to using other payments options.

We consider that appropriate safeguards through the regulation of BNPL products under the National Credit Act, in addition to allowing surcharging, would reduce consumer harm and level the playing field across the credit sector.

Open Banking and the Consumer Data Right

Additionally we note that Treasury have recently announcement an inquiry into expanding the functionality of the Consumer Data Right.[23] The Consumer Data Right will provide consumers with access to their personal financial data – in its first Open Banking iteration - giving them the power to instruct lenders to provide safe and secure access of their data to accredited third parties who will provide various services. This is currently only a "read" access right – that is the third parties will be able to read the financial data and use this data for particularly services. The new inquiry will be looking to expand this functionality to include a "write" access to enable consumers "to apply for and manage products (including, for Open Banking, by initiating payments)." This will have a potentially significant impact upon the payments system and consideration needs to be given to regulatory requirements that will need to apply to Open Banking fintechs and tools.

While we direct you to our submission to Treasury's Inquiry into Future Directions for the Consumer Data Right[24] which details the issues that will need to be considered in regulating write access, we wish to raise the following key risks of write access identified in our analysis that the Payment System Review needs to consider:

- The potential for poor consumer outcomes resulting from speedier payment and account initiation processes including more mistaken payments, lower levels of engagement with one's finances, and subsequent higher levels of debt;
- industry profiling for profit with increased economic inequality and financial exclusion as more granular data allows for finer tuned risk segmentation, and less transparent AI-informed decision-making;
- greater potential for the misuse of data including increased fraud risks, errors, incorrect advice or recommendations arising from conflicts of interest through exclusive deals,

[23] Treasurer, Building on the Consumer Data Right, 23 January 2020 https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/building-consumer-data-right

[24] https://financialrights.org.au/wp-content/uploads/2020/04/200131-CALC-submission-RBA-Payments-Review.pdf

commissions or other misaligned incentives that place the interest of the accredited third party over the best interests of the consumer.

- significant ethical issues that arise in respect of any increased functionality.
- liability and responsibility for payments made.

Concluding Remarks

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

Kind Regards,

Alexandra Kelly
Director of Casework
Financial Rights Legal Centre

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.