PO Box 16193
Collins Street West VIC 8007

29 June 2021

Australian Securities Investment Commission
By email: ePaymentsCode@asic.gov.au

Dear Madam/Sir

Consultation Paper 341—Review of the ePayments Code: Further consultation

Thank you for the opportunity to respond to Consultation Paper 341 on the review of the ePayments Code (**CP341**). The Consumers' Federation of Australia has participated in this review since its inception, having made written submissions in May 2019 and February 2021.[1] This submission is supported by CHOICE, Consumer Action Law Centre, Consumer Credit Legal Service WA, Financial Rights Legal Centre and Financial Counselling Australia.

ePayments are a substantial part of the service that banks provide to consumers, but unlike other aspects of retail banking, it is largely a utility and monopoly where consumers have little choice or ability to influence the service. For this reason, we urge ASIC to take stronger steps to ensure effective consumer protection. While we recognise that ASIC cannot make the ePayments Code (the **code**) mandatory, CFA remains of the view that it is completely inappropriate for such a fundamental service to be regulated by a voluntary code that does not meet best practice.

Our primary submission on CP341 is that we strongly object to the narrowing of the application of the code in relation to scams. Scam losses are a significant and growing problem. The ACCC's most recent report finds that there was a combined $851 million in scam losses reported to regulators and leading financial institutions in 2020, but notes that 'due to the known under-reporting of scams, we believe the financial losses referred to in this report are a fraction of the total losses suffered by Australians'.[2] In this light, the basis of any reduction of consumer protection is inconceivable.

ASIC's proposals (C3 and E1) will result in a reduction in consumer protection and a regulatory void in relation to scam losses. The proposals also appear to be contrary to ASIC's stated priorities in its

[1] See: http://consumersfederation.org.au/publications/submissions/
[2] ACCC, 'Targeting scams: report of the ACCC on scam activity 2020', June 2021, available at: https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2020.

2020-2024 Corporate Plan as well as its 2020-21 Interim Corporate Plan.[3] These documents confirm that there has been a marked increase in scams, and that disrupting scams is a priority of ASIC. For this, as well as the reasons articulated in this submission, we urge ASIC to not proceed with narrowing the application of the code in relation to scams.

This submission also provides the following responses to CP341:

- That ASIC's power to undertake targeted ad hoc compliance monitoring of the code be expanded (proposal B1);
- That the mistaken payments provisions of the code be strengthened and clarified (proposals C1, C2 and C4);
- That the unauthorised transaction provisions of the code be clarified (proposal E1);
- Various proposal to modernise terminology and operation of the code (proposals F1, F2, F3 and F4);
- That the code adopt and require the internal dispute resolution procedures of ASIC's regulatory guide 271 and that all subscribers be members of the Australian Financial Complaints Authority (AFCA) (proposal G1);
- That the expiry periods for relevant facilities are extended to 3 years in line with the gift card provisions in the Australian Consumer Law (proposal H1);
- That there are appropriate transition provisions (proposal I1).

We also suggest that ASIC consider the consumer implications of scheme card updater services, which automatically update account information on scheme cards with certain merchants.

About Consumers' Federation of Australia

The Consumers Federation of Australia (CFA) is the peak body for consumer organisations in Australia. CFA represents a diverse range of consumer organisations, including most major national consumer organisations. Our organisational members and their members represent or provide services to millions of Australian consumers.

CFA's member organisations include membership-based organisations, organisations that provide information, advice, counselling or assistance to consumers and organisations that identify regulations or market features that harm consumer interests and propose solutions. A list of CFA's organisational members is available at http://consumersfederation.org.au/members/cfa-organisational-members/

CFA advocates in the interests of Australian consumers. CFA promotes and supports members' campaigns and events, nominates and supports consumer representatives to industry and government processes, develops policy on important consumer issues and facilitates consumer participation in the development of Australian and international standards for goods and services.

CFA is a full member of Consumers International, the international peak body for the world's consumer organisations.

[3] See: https://www.asic.gov.au/about-asic/corporate-publications/asic-corporate-plan/

Proposal to reduce consumer protection in relation to scam losses

In CP341, ASIC states that "consumers should not suffer losses through mistaken internet payments and scams as a result of deficiencies in the way the industry has designed the payment instruction and processing systems". Despite this, ASIC appears to be proposing a significant reduction in consumer protection in relation to scam losses.

There are two proposals in CP341 of concern:

- That the definition of 'mistaken internet payment' be amended to ensure that it only covers actual mistakes inputting the account identifier and does not extend to payments made as a result of scams (proposal C3); and
- That the unauthorised transactions provisions only apply where a third party has made a transaction on a consumer's account without the consumer's consent and do not apply where the consumer has made the transaction themselves as a result of misunderstanding or falling victim to a scam (proposal E1).

Proposal C3

In relation to mistaken internet payments, proposal C3 will restrict the operation of the clauses 24 to 34 of the code substantially. There are many AFCA disputes where consumers who are victims of scams, such as invoice-hacking scams, subsequently seek a refund from their bank. For these disputes, AFCA applies the mistaken payments provisions of the code. It might also apply other relevant rules such as chargeback requests, where they are relevant. The focus of such an investigation is whether the institution complied with the requirements of the code, for example, whether it provided a sufficient onscreen warning pursuant to clause 25, and whether it investigated and followed the steps to seek to recover the funds pursuant to clause 27 to 30. While many AFCA disputes find in favour of the institution because it has complied with the code, this does not happen in all circumstances. The following case is an example.

Case 656981 – Bendigo & Adelaide Bank Ltd

The complainant transferred two payments from their account using an internet banking facility to purchase goods from a third party. The complainant says that they were scammed; that the third party had provided a doctored ID and bank statement and he did not receive the goods. The complainant wanted the sending bank to refund the money saying it failed to take appropriate action when he notified it of the scam later the same day.

The AFCA determination found that the transfers were mistaken payments under the code. The sending bank was liable to refund the full amount of the mistaken payments because its warning on the internet banking screen was not sufficient to displace its obligation to only pay in accordance with its customer's clear and unambiguous mandate. The transaction was processed using one part of the mandate (the account numbers) and ignoring another (the payee name) and the funds were paid into an account held in a name other than the payee. The sending bank was required to refund the payments of $2,050.

As we understand proposal C3, the above complainant would no longer receive a remedy. This is a reduction in consumer protection and thus should be rejected outright.

ASIC's reasoning for proposal C3 states that detecting and responding to scams involves a range of considerations and processes, and that industry processes are different to current mistaken internet payment processes. It states that 'if scams were to be addressed through the code, it would need to be through a set of bespoke rules, modelled on current industry practice to address instances in which a consumer has made a payment in response to a scam, not through the MIP framework'. ASIC does not, however, propose a set of rules inside or outside this code. As such, if ASIC's proposal proceeds, consumer protection will be reduced and there will be an absence of clear rules or consumer entitlements, leaving consumers at mercy of industry practice. While industry has taken some steps to address scam conduct, actions are not transparent and the lack of any standard gives no certainty that consumers are treated consistently in accordance with best practice.

ASIC also states that it will not use the code to require an account name and number matching requirement for 'pay anyone' transactions using a BSB and account number. We note that this position is at odds with other consumer affairs officials, such as the WA Commissioner for Consumer Protection[4] and the ACCC.[5] While we recognise that the legacy payment infrastructure system BECS is being replaced with the New Payment Platform (NPP) which has greater capability around account matching, the industry has been very slow in rolling out this technology.[6] In this light, there is little justification in reducing consumer protection. Furthermore, the proposal would seem to reduce the incentives for industry to better protect their customers through quicker uptake of the NPP by reducing the likelihood that institutions will be found liable for scam losses.

Payment redirection scams appear to be on the rise. The ACCC's scam watch report found that payment redirection scam losses amounted to $128 million in 2020.[7] We simply don't understand why ASIC would seek to reduce the limited standards that apply to protect against this level of consumer losses.

Proposal E1

In relation to proposal E1, we are 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 fact controlled by a scammer. A common example might be a romance-based scam, or even investment scams, where the fraud generally arises following a relationship where there is an implication of trust. In essence, the scammer grooms the consumer and, based on trust that develops, engages in improper exploitation of the use of funds of the consumer. We consider that in some circumstances, such transactions can be said to be unauthorised, in the sense that the consumer was under the undue influence of the scammer and did not truly authorise the transaction for the purpose they believed it to be for. This is not dissimilar to certain remote access scams where the consumer has not made the transaction themselves—ASIC agrees that the consumer did not authorise such transactions and thus the unauthorised transaction provisions of the code should apply to determine liability.

[4] See: https://www.abc.net.au/news/2021-03-17/aged-care-resident-scammed-out-of-bond-in-375000-email-hack/13226362
[5] ACCC, above n 2, page 18.
[6] RBA, 'New Payments Platform Functionality and Access: Conclusions Paper', June 2019, available at: https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/functionality-and-access-report.html
[7] ACCC, above n 2, page 8.

ASIC proposes to amend the unauthorised transaction provisions of the code to 'clarify' that they do not apply where the consumer has made the transaction themselves as a result of misunderstanding or falling victim to a scam. We consider that this is a step backwards in terms of consumer protection and oppose the recommendation.

We acknowledge that AFCA does not often consider transactions made as a result of trust-based scams to be unauthorised, but we consider that this is not always a correct interpretation of the law. As noted above, we consider trust-based scams like romance scams, investment scams and remote access scams to be alike, and therefore should be treated similarly. Furthermore, we consider that our interpretation is aligned with good public policy—it is appropriate that financial firms bear greater liability for these sorts of scams given they are in a much better position to identify fraud risk and invest in capabilities to mitigate such risk. We note that there are a range of relevant legal principles that place duties on financial firms. For example:

- Firms regulated by AUSTRAC are required to monitor customer transactions, including unusually large transactions, complex transactions and unexpected patterns of transaction that do not seem to have a legitimate purpose. The primary purpose of these obligations is to protect against criminal activity, which includes fraudulent scam activity.
- Implied warranties in a customer-firm contract impose a duty to exercise due care and skill.[8] In a UK decision, it was stated in relation to a duty of care on bankers that 'the law should guard against the facilitation of fraud, and exact a reasonable standard of care in order to combat fraud and protect bank customers and innocent third parties'.[9]
- The obligation on firms to conduct services 'efficiently, honestly and fairly'[10] has been given more emphasis since the Royal Commission into Misconduct into the Banking, Superannuation and Financial Services Industry. As stated by the Commissioner, 'understood properly, this requirement would embrace all six norms of conduct [identified by the Royal Commission]'. While we are not aware of any case law that has applied this obligation in relation to unauthorised transactions, it would be appropriate that changes to the code be developed consistent with this duty.
- The Code of Banking Practice, including the promise to engage in a fair, reasonable and ethical manner,[11] and the Australian Banking Association industry guideline, 'Protecting vulnerable customers from financial abuse' are also relevant instruments.[12]

We urge ASIC to reconsider its proposal to ensure that there is a greater obligation on financial firms to protect consumers in relation to scams.

Regulatory void in relation to scams

Should ASIC proceed with its proposals that limit the application of the code to scam transactions, there will be a regulatory void in relation to scams at the very moment when scams are on the rise.

ASIC needs to recognise that consumers can only protect themselves up to a point, and that reliance on industry practices to protect against scams risks ASIC's vision of fair, strong and efficient financial

[8] Section 12ED, *Australian Securities & Investments Commission Act 2001*.
[9] *Barclays Bank plc v Quincecare Ltd* [1992]4 All ER 363 at 376
[10] Section 912, *Corporations Act 2001;* Section 47, *National Consumer Credit Protection Act 2010*.
[11] Clause 10, Code of Banking Practice.
[12] ABA, Preventing and responding to financial abuse (including elder financial abuse), April 2021, available at: https://www.ausbanking.org.au/banks-unite-to-help-customers-experiencing-financial-abuse/.

system. CFA considers that financial institutions should shoulder more responsibility for money lost to scams made by internet transfer, just as they generally reimburse customers who lose money due to scams via unauthorised card transactions or other fraudulent account activity. Institutions will then have an incentive to use technology and information, in ways that consumers simply cannot, to develop better mechanisms and prevent the fraud occurring in the first place.

For this reason, CFA cannot support the proposals and could only support changes to the code should there be developed, and in force, an alternative regulatory framework to better protect against scam losses.

We note that, in the UK, banks and consumer groups have developed a voluntary industry code, known as the Contingent Reimbursement Model (CRM) Code, to reduce both the occurrence and impact of 'authorised push-payment scams'.[13] The CRM code seeks to provide confidence to people that, if they fall victim to such a scam and have acted appropriately, they will be reimbursed.

The CRM code states that where a customer has been the victim of a relevant scam, signatory firms should reimburse the customer, subject to some exceptions (including relating to a customer taking the requisite level of care). There is also a "no blame" fund which signatories contribute to that can cover the costs of reimbursement.

A recent review of the CRM code shows that average reimbursement rates have risen from around 20% to 45% and banks have invested more heavily in warnings on their apps and online banking systems.[14] Some institutions have introduced (either voluntarily or after being directed by the regulator) systems such as Confirmation of Payee to help people spot when they may be making a payment to the wrong account. While, as a voluntary code, it does suffer from 'haphazard and inconsistent implementation by signatories', a range of recommendations have been made for improvement:

- a wider range of participants in the payments system should be part of it;
- the type of scams it covers should be extended beyond where consumer pushes funds to the scammer, to pushing via a range payment methods within the scam;
- new governance and oversight processes; and
- better reporting and data.

CFA recommends that, before any changes are made to the code, a more comprehensive and fairer regulatory instrument be enacted that better protects consumers from scams. This needs to specifically respond to the issue of consumer vulnerability, noting that older people and people from non-English speaking backgrounds are disproportionately represented in scam losses.[15]

Ensuring the code aligns with general law

Any regulatory instrument needs to reflect and build on the general law. The CFA holds long-standing concerns that the code's regime for mistaken payments does not reflect the law.

---

[13] Lending Standards Board, Contingent Reimbursement Code, available at: https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/

[14] Which?, The CRM Code: two years on, May 2021, available at: https://conversation.which.co.uk/scams/contingent-reimbursement-model-code-two-year-anniversary/

[15] ACCC, Media Release: Culturally and linguistically diverse community lose $22 million to scams in 2020, reports from Indigenous Australians up by 25 per cent, 10 June 2021.

Furthermore, the general law has evolved since the code was last reviewed, and this has not been acknowledged.

The current position in Australian law regarding mistaken payments was set out by the High Court in *David Securities v Commonwealth Bank of Australia* [1992] HCA 48, where the court agreed with the statement that: "Mistake not only signifies a positive belief in the existence of something which does not exist but also may include 'sheer ignorance' of something relevant to the transaction in hand".

The court made it clear that the cause of the mistake—whether in fact or law—is not relevant to whether a right of recovery arises. The relevant consideration is that the payer has made a payment to an unintended payee. How this has been done (transposition error, being provided with the wrong account number, on the basis of an unfounded belief) does not affect the existence of this right.

"Mistake" can take a variety of forms, for example, an incorrect belief that an amount is owed under law or pursuant to a contract. Or it can be a transposition mistake, where an incorrect account number is entered as part of an online payment. Or it can be where account details are erroneously substituted due to fraud, as in the case of invoice scams. Indeed, in the case of *Australian Financial Services and Leasing Pty Ltd v Hills Industries Ltd* [2014] HCA 14, the High Court recognised that prima facie right of recovery arose from a payment made pursuant to invoice fraud. Negligence on the part of the payer is not relevant to whether a right of recovery arises, only that it is the mistake that caused the transfer.

The code should be consistent with the general law as it currently stands in Australia. Any diversion which further undermines consumers' right of recovery is inconsistent with ASIC's own guidance on approval of industry codes, which expects codes to complement and exceed existing obligations.[16] Proposal C3, referred to above, would result in lower protection than is available to consumers at law, without justification other than what is more convenient for industry.

If a consumer claims to their bank that they have sent funds to an unintended recipient, whatever the reason, they have prima facie right of recovery which their bank should act on, and *Australian Financial Services Leasing Pty Ltd v Hills Industries Ltd* confirms that this includes instances where the payment is induced by fraud.

Making complaints against receiving institutions

At paragraph 58 of CP 341, ASIC states that it considered whether the AFCA Rules should be amended to enable determinations against a receiving ADI in relation to mistaken payment disputes. However, ultimately, ASIC considered it inappropriate to allow complaints against the receiving institution because the receiving institution does not have contractual obligations to the consumer who made the mistaken internet payment.

CFA strongly rejects this decision and considers that the current gap in AFCA Rules creates a significant access to justice issue. CFA members regularly advise consumers about their rights under the code with respect to mistaken payments and are frustrated that the obligations on receiving

[16] ASIC, RG 183: Approval of financial services codes, para 183.22, available at: https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-183-approval-of-financial-services-sector-codes-of-conduct/.

institutions are not enforceable at AFCA. It may be that the sending institution has done all it can do, but the receiving institution has not, for example, returned funds to the sending institution as required by the code. In these instances, AFCA considers it cannot consider complaints against the receiving institution because it has not provided a financial service to the complainant. We consider that there is little point putting obligations on receiving institutions if they are not enforceable by the consumer. We note that ASIC rarely takes enforcement action in relation to non-compliance with the code, so any enforcement is generally the burden of the consumer through complaints.

Moreover, CFA does not consider that the fact that the receiving institution does not have contractual obligations to the consumer who made the mistaken internet payment should preclude a complaint. There are a range of complaints that can be made at AFCA outside the provision of a contractual obligation. For example:

- entitlement or benefits under a life insurance or general insurance policy – see rules B.2.1 (c) and (d);
- a legal or beneficial interest arising out of a financial investment or similar risk product – see rule B.2.1 (e);
- a claim under another person's motor vehicle insurance product for property damage to an uninsured motor vehicle caused by a driver of the insured vehicle – see rule B.2.1 (f);
- breach of obligations arising from the Privacy Act or the Consumer Data Framework – see rule B.2.1 (i); and
- prospective consumers are entitled to rely on commitments made under the Banking Code of Practice – see chapter 1, definition of 'you'.

There is no reason why AFCA Rules could not be amended to make it clear that a consumer can make a complaint against a receiving institution in relation to mistaken internet payments, and we urge ASIC to reconsider its position.

Other proposals in CP 341

The below summarises our position in relation to various of the other proposals made in CP 341.

- Proposal B1 on compliance monitoring – CFA considers that the code should empower ASIC to collect a range of industry data to inform compliance and its regulatory objectives. This should include an ability to collect data on an ongoing basis, not just one-off. In this vein, we encourage ASIC to establish automatic data collection using RegTech as it has in the life insurance sector. We understand that ASIC has undertaken consumer research about payments issues including unauthorised transactions during 2020. We encourage ASIC to publish this research to inform community understanding and policy dialogue.

  We also note that the five questions in the consultation paper relating to proposal B1 focus primarily on the costs to industry of data collection and compliance monitoring. ASIC should be also considering the benefits of data collection, not solely the costs. The Commonwealth's guidance for regulatory impact analysis states: 'Comparing the costs and benefits of each proposed option requires rigorous and logical analysis in support of the RIS conclusion. Assess the net benefit—overall benefit minus costs—to the current status

quo.'[17] There will be a risk of not correctly identifying net benefit where agencies seek input on costs, but not the benefits of a proposal or regulatory option.

- Proposals C1, C2 and C4 on mistaken internet payments – in relation to proposal C1, CFA supports clearer obligations on receiving institutions to return only a portion of the funds in an account if that is all that is available. This is fair and ensures some level of redress. We also support the code clarifying the reasonable endeavours that a firm should undertake to retrieve funds. We consider that further consultation should be undertaken about the development of this guidance.

- In relation to proposal C2, we support the code clarifying the time frame for the sending institutions to request the funds be returned, but we consider that 5 days is too long. In many cases, the funds will be gone in this time frame. Given the low-cost of electronic transactions and requests, we consider that this should be reduced to 1-2 days. We support improved requirements around record-keeping to enable more efficient complaints and dispute processes. As noted above, we strongly oppose the proposal that will limit complaints against receiving institutions.

- In relation to proposal C4, we generally support the proposal for enhanced on-screen warnings in relation to the risks associated with mistaken payments, however, we do not consider that this is sufficient consumer protection. In CP 341, ASIC references its own research on the limitations of consumer warnings.[18] Recent research confirms that information remedies often do not work to protect and empower consumers, even when consumers would get a financial benefit.[19] So it is disappointing for this proposal to be recommended as a primary form of consumer protection. ASIC also notes that it would like to see NPP's PayID service more actively promoted, given this service includes a confirmation step before the payment is made so users can check they are paying the right person or business. We think ASIC should go further and require institutions to conduct all 'Pay Anyone' transactions via this service or, at the very least, require institutions to offer this service as the default.

- In relation to other aspects of proposal E1 on unauthorised transactions, we support clarification that a code signatory must prove that the consumer's breach of the pass code security requirements contributed to the loss before an institution can deny liability. We also support clarification that the unauthorised transaction regime of the code is distinct to, and separate from, card scheme chargeback arrangements.

[17] Department of Prime Minister & Cabinet, *Regulatory Impact Analysis Guide for Ministers' Meetings and National Standard Setting Bodies*, May 2021, available at: https://pmc.gov.au/resource-centre/regulation/regulatory-impact-analysis-guide-ministers-meetings-national-standard-setting-bodies

[18] ASIC, REP 632 Disclosure: Why it shouldn't be the default, May 2019, available at: https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/.

[19] Adams et al, 'Testing the effectiveness of consumer financial disclosure: Experimental evidence from savings accounts', *Journal of Financial Economics*, March 2021.

- In relation to screen scraping, we refer to and support the prior submission from Financial Rights Legal Centre on this issue.[20] We note that ASIC states that there are interpretations of the code that state that inputting one's pass code into a screen scraping service does not amount to 'disclosure' of the pass code, and therefore is not a breach of the code's pass code security requirements. If ASIC is proposing to provide protection to consumers from losses in this regard, then the code needs to clearly state that inputting one's pass code into a screen scraping service will not result in consumer losing their entitlements under the code—it is not clear to us that ASIC's proposal is providing this level of clarity. To clarify, we agree with ASIC that sharing pass codes is a risky activity and we do not consider that screen scraping services should be able to operate outside the safeguards of the Consumer Data Right framework.

- In relation to proposals relating to modernising the code, CFA supports updating the code so that it responds to biometric authentication that is commonly used by personal devices (proposal F1). We also support revising the term 'device' in the code and instead refer to 'payment instrument' (proposal F2) and extending all provisions relevant to 'Pay Anyone' transactions to include NPP transactions (proposal F3).

- In relation to proposal G1, we strongly support updating regulatory requirements in the code relating to internal and external dispute resolution, including referencing the updated Regulatory Guide 271 and requiring all subscribers to be members to AFCA.

- In relation to proposal H1, we welcome the proposal to align the facility expiry period in the code with the expiry period for gift cards in the Australian Consumer Law, which is 36 months.

- In relation to transition (proposal I1), we generally support the proposal for a transition period but we consider that it should be a relatively short period, i.e. no more than 6 months, after ASIC's final decision on the policy positions pursuant to the current review. We note that this review has been going on for more than 2 years and that the code is severely overdue for updating and renewal.

Card scheme updater services and recurrent payments

CFA notes that some card schemes are offering 'updater services' whereby the scheme will update merchants who hold recurrent payments arrangements on scheme cards whenever the card is expired or replaced.[21] This service may be convenient for some people who forget to update merchants with new account information changes, and may avoid payments not being made on time.

However, such a service may also negatively affect some people experiencing vulnerability and disadvantage, by limiting control over the level and timing of recurrent payments. For example, where people are scammed, appropriate advice may be to have a new card issued. However, if

[20] Financial Rights Legal Centre, submission available at: https://financialrights.org.au/wp-content/uploads/2021/04/210118_ePaymentsCodeProposal_Letter_FINAL.pdf.
[21] See: https://www.visa.com.au/dam/VCOM/global/run-your-business/documents/vau-merchants.pdf

recurring charges are allowed to continue on a card with a new expiry date, this will not protect the customer. It appears that losses have been incurred overseas as a result of these arrangements.[22] We consider that these updater schemes should only be allowed where the consumer has actively opted-in to the service, not as a default, and encourage ASIC to investigate this issue and update payments regulation as appropriate.

CFA also considers that the code could be enhanced to give consumers the right to cancel recurrent payments on scheme cards. Chapter 34 of the Code of Banking Practice provides that signatory banks will cancel a direct debit request promptly. This does not, however, extend to recurrent payments on scheme cards. This gives rise to inconsistent rights, confusion for consumers, and can result in financial harm where a merchant refuses unreasonably to cancel the recurrent payment.

Final comments

We urge ASIC not to proceed with its current review, outside making any minor essential updates to the code. Rather, ASIC should establish a new and more substantial project to tackle the regulation of ePayments and scams, in a way that might gain the confidence of consumers not just the banking and payments industry.

Should you wish to discuss this submission, please contact us at info@consumersfederaton.org.au.

Yours sincerely

Chairperson

[22] See: https://www.stuff.co.nz/business/money/113589581/how-hackers-used-creditcard-feature-to-defraud-us-woman-199-at-a-time