cclswa

# ASIC Consultation Paper 341: Review of the ePayments Code: Further consultation

Submissions by Consumer Credit Legal Service (WA) Inc.

July 2021

Consumer Credit Legal Service (WA) Inc
Level 1, 231 Adelaide Terrace, Perth WA 6000
Phone (08) 9221 7066 Fax (08) 9221 7088
Email info@cclswa.org.au
www.cclswa.org.au

ABN 43 262 474 001

# Contents

# 1 Introduction

The Consumer Credit Legal Service (WA) Inc. (**CCLSWA**) takes the opportunity to provide submissions to the ASIC Consultation Paper 341: Review of the ePayments Code: Further consultation (**CP 341**).

## About CCLSWA

CCLSWA is a not-for-profit specialist community legal centre based in Perth. CCLSWA operates a free telephone advice line service which allows consumers across Western Australia to obtain information and legal advice in the areas of banking and finance, and consumer law. CCLSWA also provides ongoing legal assistance to consumers by opening case files when the legal issues are complex and CCLSWA has capacity to do so.

CCLSWA's mission is to strengthen the consumer voice in Western Australia by advocating for, and educating people about, consumer and financial, rights and responsibilities.

In the 2020/2021 financial year, CCLSWA noted a marked increase in the advice provided through our telephone advice line that referenced the ePayments Code (**Code**), more particularly unauthorised transactions and mistaken internet payments. Around half of our calls regarding the Code related to consumers trying to recover funds lost as a result of scams.

In the past year, CCLSWA also opened case files and represented several clients seeking redress under the Code. Most of these matters related to clients who were victims of scams and seeking redress under the Code's unauthorised transactions provisions. In contrast, only one case file client in the past year had a mistaken internet payment matter (and not a scam).

CCLSWA also provides community legal education programmes relating to credit and debt issues. Feedback from sessions delivered to high school students and older people's groups indicates that online scams are a real concern to these groups.

It is for these reasons that CCLSWA is well placed to respond to ASIC's review of the Code in CP 341. In addition, we would like to take this opportunity to voice our concerns regarding the adverse impact on consumers of certain proposed changes to the Code by CP 341.

In these submissions CCLSWA draws on its experience to form a view and make recommendations as to how the Code may be strengthened and continue provide important consumer protections.

We have incorporated case studies as examples of our experience. In most of these case studies, we have not named the Code subscribers. We have made these entities anonymous to protect our clients' confidentiality. We have not used our client's real names. We have also made some of the entities anonymous as some matters are ongoing and others are subject to confidentiality agreements. If ASIC would like to know the name of a subscriber or further detail on a particular case study, CCLSWA can approach the relevant client and seek his or her permission for those details to be provided.

# 2 Overview

2.1 Our key concern with the proposed changes to the Code is that consumers will no longer have an avenue for redress where they have been victim of certain types of scams, through either the Code's mistaken internet payment, or unauthorised transaction provisions.

2.2 ASIC's stated purpose of the review, at paragraph 7 of CP 341, is "…*to ensure (a) the policy settings in the Code are appropriately positioned for today's – and to the extent tomorrow's—consumers and electronic payments service providers; and (b) the Code is simple to apply and easy to understand for both subscribers and consumers*."

2.3 In an increasingly digitised consumer environment, spurred by a global pandemic, Australian consumers are experiencing higher than usual financial and personal information loss as a result of scams[1] Accordingly, we do not consider the proposed changes to narrow the applicability of the Code to scams to be "appropriately positioned" for today or tomorrow's consumers, in the absence of any other protections for scam victims being introduced.

2.4 CCLSWA would welcome the opportunity to consult further with ASIC in relation to regulating scams through new legislation, regulatory guidance, or industry code, but in the interim urge ASIC not to remove consumer access to existing avenues for redress. Without the current Code provisions, there would be no clear pathway for redress for consumers who are victims of certain online banking and payment scams, such as authorised push payment scams (where a consumer is tricked into transferring funds to a scammer's account).

2.5 We agree that the Code should ideally be simple. The Code is currently difficult to navigate and interpret, particularly for consumers who may not be financially literate. However, we cannot agree with the proposed changes in CP 341 sections C3 and E1.

2.6 If ASIC were empowered in the future to make compliance with the Code mandatory and substantially redraft the Code, we would welcome an alternative, consumer friendly framework to regulate scams.

2.7 Our submissions below are limited to address the sections of CP 341 which fall within the scope of our experience as consumer advocates and community lawyers. We have endeavoured to respond to ASIC's specific questions, but our deep concern and the focus of these submissions is the proposed removal of certain scams from the Code, at CP 341, sections C3 and E1.

[1] Targeting scams - report of the ACCC on scams activity 2020 v2.pdf

# 3 Part C: Clarifying and enhancing the mistaken internet payments framework

## Partial return of funds

| |
|---|
| C1Q1 Are there any special considerations to justify not applying the processes in clauses 28, 29 and 30 to situations in which only partial funds are available in the unintended recipient's account? |

3.1 CCLSWA is not aware of any special considerations that would justify not applying the processes as set out to situations where only partial funds are available from the unintended recipient's accounts.

| |
|---|
| C1Q2 Are there benefits in applying the MIP framework to situations where only partial funds are available for return? Please describe these benefits |

3.2 CCLSWA believes that there is considerable benefit to consumers in applying the mistaken internet payment (**MIP**) framework to situations where there are only partial funds to return.

3.3 The clear benefit for consumers is that they can recoup at least some of their losses, as compared to potentially not being able to recover any funds, if they have to wait for full sufficient funds to appear in the unintended recipient's account.

3.4 The ability to recoup partial funds has the potential to limit the ripple effect such financial loss can have by alleviating some of the practical hardships that the consumers may otherwise encounter from the loss of funds.

3.5 Further, we support ASIC's rationale that recipients of unauthorised transactions should be aware that they are not entitled to the funds.

3.6 We agree with ASIC that it should not cause any increased effort on the part of subscribers to recover partial funds in circumstances where they are required in any event to undertake the investigative process for retrieval of the consumer's funds from a MIP.

3.7 CCLSWA would like to see that the MIP framework for subscribers continuing and extending to partial return of funds.

3.8 Marina's story below is illustrative of the types of consumers CCLSWA assists with advice on how to report a MIP.

**Marina's story**

Marina works part time and earns a low income.

In December 2020, Marina made a transfer of $2500 from her bank account to another bank account at a different bank.

She realised immediately after the transfer was made that she had incorrectly entered the last two numbers of the account.

She contacted her bank on the same day the transfer was made. She was told by her bank that she had to wait for the transfer to clear before she could dispute it.

After the funds cleared, Marina contacted her bank and was told it would take 45 days to get an outcome.

After 45 days, she was contacted by her bank, and told it could not retrieve the money, and to report it to the police. The police informed her that it was a civil matter and referred her to CCLSWA for assistance.

Marina said that the payment was "not a small amount of money to her".

3.9 For Marina, if there had been the option for a return of at least partial funds, whilst an investigation is ongoing, it may have alleviated any financial strain the loss of the funds put on her.

3.10 Marina's case study is also illustrative of the importance of acting on a report of a MIP without delay, and the need for frontline staff training on the Code, as discussed in more detail below.

C1Q3 Do you think it would be useful for the Code to provide a non-exhaustive examples of what might amount to "reasonable endeavours"? If not, why not?

3.11 CCLSWA supports the inclusion of a non-exhaustive list of examples of what might amount to "reasonable endeavours".

3.12 We wish to emphasise to ASIC that it is vital to make clear to subscribers that any examples provided are non-exhaustive, are for guidance only, and do not represent a 'minimum standard' for subscribers to follow.

3.13 CCLSWA has concerns that if subscribers are provided with a list, they will see this as a 'safe harbour' whereby they can take those steps, and only those steps to comply with their obligations under the Code.

C1Q4 What types of examples would be helpful in a non-exhaustive list of examples of what might amount to "reasonable endeavours"?

3.14 We note that there are already provisions under the current Code for the 'receiving ADI' to set up a payment by instalment to recover the mistakenly transferred funds[2]. We consider that this is an appropriate step that subscribers are already required to undertake and as such should be included in any list of examples of reasonable endeavours to recover funds.

3.15 As part of the process for recovering MIP at section 29.3(a) of the Code, there is also a requirement for the 'receiving ADI' to prevent the unintended recipient from withdrawing funds for a further 10 business days. In the event that the unintended recipient does not establish their entitlement to the MIP funds, the funds will be withdrawn from the recipient's account and returned via the 'sending ADI'.

3.16 We consider that this can be included in any further list of "reasonable endeavours".

3.17 CCLSWA considers that there may be scope for the Code to go further in this regard, particularly in the contexts of scams, to freeze funds where the funds have been transferred again, after arriving in the first account of the unintended recipient to other accounts with the same receiving ADI.

3.18 Further, we consider that there should be more than one attempt made to retrieve funds. We consider that a minimum of 2-3 attempts would usually constitute reasonable attempts to retrieve funds.

3.19 Again, we emphasise that any list of examples is non-exhaustive and does not represent a "minimum standard".

C1Q5 What types of factors might affect whether a particular action is necessary to satisfy 'reasonable endeavours' in individual cases?

3.20 CCLSWA considers a "reasonable consumer" test like that applied under *Australian Consumer Law* (ACL) may be useful to determine relevant factors for justifying whether particular action is necessary to satisfy 'reasonable endeavours'. Similarly to the ACL, relevant factors may include the amount of the transfer, the purpose of the transfer and any factors that indicate if the customer is vulnerable.

3.21 The amount of funds that have been mistakenly transferred may be relevant to what would be considered reasonable endeavours to retrieve the funds. However, this is not to diminish the impact of relatively low value transfers. Rather, it may be particularly relevant to highlighting consumer vulnerabilities where the transferred amount represents a significant

[2] Section 32.1 of the Code.

proportion of the consumer's total available funds. This may be indicative of the resultant financial hardship experienced by the consumer because of the MIP.

3.22 While ASIC is proposing to remove scams from the definition of MIP (see our submission below responding to C3 at page 14) we consider the purpose of the funds transfer to be another relevant factor that can impact on whether a particular action or actions are required to satisfy a 'reasonable endeavours' test. We maintain that a consumer who was deliberately directed to complete a transfer for a purpose the recipient could not fulfil, would reasonably expect to have their funds refunded. The purpose may also reveal particular vulnerabilities and be indicative of the extent of the impact of the MIP on the consumer.

3.23 Regulators are aware that scammers try to target consumers who are more susceptible, for example, by reason of their language skills or cultural background. CCLSWA's position is that customer vulnerability should be a consideration for a consumer who has transferred the MIP. ASIC may wish to consider this factor also applying to the unintended recipient.

3.24 CCLSWA regularly assists consumers who are experiencing financial difficulty. We are concerned about situations where a vulnerable consumer is the unintended recipient of funds and have subsequently spent the funds without realising their rights and obligations in relation to those funds.

3.25 We reiterate our concerns that any list of factors or list of examples included in the Code must be clearly identified as non-exhaustive and not a minimum standard.

| C1Q7 What are the costs to subscribers of extending the MIP framework to cover the partial return of funds? |
|---|

3.26 CCLSWA cannot provide submissions on the costs to subscribers in extending the MIP framework to cover partial returns of funds.

3.27 However, we presume there would not be any increased investigative burden on subscribers, given subscribers are already required to take steps to investigate and recover funds from a MIP.

3.28 We would also consider any nominal additional cost resulting from extending the MIP to cover partial return of funds would be outweighed by the overall benefit to consumers of having those funds returned to them.

## Responsibilities of the sending and receiving ADIs

C2Q1 Do you agree with the proposed timeframe in proposal C2(a)? If not, why not?

3.29 CCLSWA agrees that there must be a set timeframe for sending ADIs to investigate reports of MIPs. This is an important protection for consumers that currently does not exist in the Code. In contrast, we note the Code has strict reporting timeframes for consumers who mistakenly transfer a payment and fairness dictates that such strict requirements be reciprocated.

3.30 As for the specific timeframe proposed, we consider that the sending ADI is well placed to respond quickly, and the speed with which funds may be transferred between accounts and ADI's demands a quick response. Accordingly, we maintain that 5 business days is too long a period to allow a sending ADI to investigate and request the return of funds from the receiving ADI. CCLSWA considers subscribers should have adequate systems and procedures in place to easily investigate and report a MIP transaction within a shorter timeframe of 1-2 business days. It follows logically that the sooner the investigative process begins, the greater the likelihood of the consumer recovering the funds.

3.31 We have advised several clients who have been disadvantaged by subscribers delaying their steps to investigate and attempt to recover a MIP.

3.32 CCLSWA notes that most callers to our telephone advice line regarding MIP instruct that the sending ADI has not given them clear guidance about the recovery process, and there has been a consistent failure by both the sending and receiving ADIs to adopt the required investigative mechanisms and processes and comply with the timelines prescribed under the Code.

3.33 Liam's story, below, illustrates the difficulty for consumers in recovering funds due to delays by the sending ADI to commence the investigation of a MIP.

**Liam's story**

English is not Liam's first language, and he required the assistance of an interpreter to instruct CCLSWA.

In early June 2020 Liam intended to transfer $2,000 from his bank account to his wife 's bank account (with a different bank), to allow her to pay training fees.

Liam made the transfer through his mobile banking app via the 'Pay Someone' function, and by user error selected a BSB and Account Number that did not belong to his wife.

Two days after making the transfer, Liam became aware that he had transferred the money to the wrong bank account. It transpired that the MIP was made to another recipient account at Liam's bank.

On the same day, Liam contacted his bank by phone to report the MIP and seek to have the funds returned, using an interpreter. He was told by the bank that the payment investigation would take 45 days.

Some 41 days later after having reported the MIP to his bank Liam still had not received a response, so he attended his local bank branch to enquire. Subsequently, and on the same date, he received a message from the bank stating:

'*I apologise for any delay and can assure you that the correct procedure is being followed. Due to system error, the initial case was not successful, but I have reopened a new case for you.*'

Some 81 days after the MIP, Liam received a further note from his bank stating:

'*We have made attempts to contact the person who received the money and asked them to return it. Unfortunately, we have been unsuccessful in the recovery of these funds.*'

In around October 2020, on behalf of Liam, CCLSWA wrote to the bank advising that it had breached the Code and seeking reimbursement of the payment.

The matter was subsequently resolved.

3.34 Liam's case study highlights a subscriber's failure to acknowledge the receipt of a mistaken internet payment report, failure to comply with the timeframes of the Code and failure to notify the consumer of the outcome of the complaint. While Liam was ultimately credited $2000, he was not compensated for the stress or inconvenience caused by his bank's failures. We hold concerns for unrepresented consumers in similar scenarios, especially those facing language barriers like Liam.

3.35 Based on our work with Liam, and other clients' complaints of delay, we strongly support ASIC's proposed change to set a strict timeframe for sending ADIs to investigate and report a MIP.

3.36 We also request that as part of the work ASIC undertakes to implement any Code revisions, ASIC review subscribers' processes and procedures and ensure that their front-line staff are trained to give genuine consideration to a customer's MIP and are aware of their obligations under the Code, particularly regarding their role in starting the process to investigate and report an MIP. We also note that many older, and culturally and linguistically diverse consumers appear to preference face to face branch contact, as in Liam's case, so it is important that they receive appropriate attention and information from the staff they encounter there.

3.37 CCLSWA is often called by consumers who, upon reporting a MIP, have been told by their bank that the funds need to clear first, or that they should wait to see if the funds bounce back before making a report. This is concerning and supports our call for better training of

front-line staff. Any delay in the reporting of MIP has a significant impact on the consumer's ability to recover their funds.

3.38 CCLSWA supports the imposition of a strict timeframe, of ideally 1-2 business days, for the sending ADI to act and report any MIP.

C2Q2 What are the costs associated with compliance with the proposed timeframe?

3.39 CCLSWA cannot comment on the costs to industry associated with compliance with timeframes, however we consider that any costs would not be greater than the personal and financial ramifications for consumers who cannot recover their MIP because of delayed action by their bank.

C2Q3 Do you agree with the proposed recording keeping requirements? Why or why not? What are the costs of the proposed record keeping requirements?

3.40 We support ASIC's proposal requiring subscribers to keep 'reasonable records' of the steps they took and what they considered in their investigations into MIPs. However, where there are requirements to keep records, we suggest that it would be useful if ASIC prescribed some minimum standards for record keeping. Prescribing a minimum standard for record keeping would ensure that information is consistent for all subscribers.

3.41 Additionally, the Code should require the sending ADI to make investigative records available to consumers when telling them the outcome. This would assist the consumer formulate any further complaint to the ADI or AFCA.

3.42 CCLSWA considers that consistent records and access to information across all subscribers would improve efficacy and access to justice.

3.43 We consider that subscribers, at a minimum, should record information such as the date/time the MIP was reported to the sending ADI, steps taken by the sending ADI to investigate, including timing when correspondence with the receiving ADI was sent, its general contents, results of any investigation and documents relating to any decisions and rationale, and details of any escalation and records of communication with the consumer whether over the telephone or in writing.

3.44 Liam's story above demonstrates the importance of minimum standards of record keeping for consumers under the Code's MIP provisions. In Liam's story, he used the telephone to report his MIP using a translator, and his bank failed to act on this report. Generally, it is easier for clients with English as a second language, to communicate verbally using a translator, than in writing. However, negative inference can be drawn from the lack of

written communication if a dispute escalates. Liam did not understand why his bank was taking so long to recover the funds.

3.45 We consider that clear record keeping of telephone calls, as well as written correspondence, is vital to ensure vulnerable consumers are protected when MIP investigations are delayed, or not conducted properly.

C2Q4 What do you consider are the costs of requiring ADIs to inform consumers of their dispute resolution rights?

3.46 As Code subscribers are already required to tell the consumers the outcome of their complaints, CCLSWA considers that there would be no or minimal increased costs to subscribers to also inform consumers of their dispute resolution rights in the same correspondence.

3.47 We would consider it good industry practice for subscribers to include information about how to complain to the sending ADI and then, if appropriate, AFCA in any relevant correspondence with consumers about an investigative outcome.

3.48 We strongly support the inclusion of consumer dispute resolution rights in any correspondence to consumers regarding the outcome of a MIP investigation, and do not consider the cost of including this information would be onerous on subscribers.

C2Q5 What are the benefits and/or burdens of C2(d)? How do they compare to benefits and/or burdens of the current requirements in the Code?

3.49 CCLSWA disagrees with ASIC's conclusion that a 'receiving ADI' should not be subject to a complaint from the consumer who made the MIP. We do not consider that a lack of contractual relationship between the parties should be a barrier to consumers making a complaint in situations where a 'receiving ADI' has failed to meet its obligations under the Code.

3.50 CCLSWA generally agrees that the 'sending ADI' should not be held accountable for the failures of the 'receiving ADI' or the unintended recipient's refusal to return funds. We consider, however, that there must be a clear avenue for recourse for consumers where the failure to retrieve funds has resulted from the 'receiving ADI's' failure to comply with their obligations under the Code.

3.51 This issue is demonstrated by Jane's story, below, where the receiving ADI failed to comply with the Code. CCLSWA assisted Jane to lodge a complaint against Jane's bank to retrieve funds (although Jane's bank had appeared to comply with its obligations as the sending ADI),

and it was only through persistence and advocacy that we could obtain an outcome for Jane from the receiving ADI.

3.52 We disagree with ASIC's view that AFCA should not be permitted to make determinations against a receiving ADI for failure to cooperate.

3.53 We consider that AFCA's Rules should allow the receiving ADI to be joined to any AFCA complaint regarding MIP and further allow consumers to bring a complaint solely about a receiving ADI's misconduct, where that bank has failed to comply with its MIP Code obligations.

3.54 While we understand ASIC's concern that the receiving ADI is not contractually bound to the consumer bringing a complaint, we consider that AFCA's jurisdiction for certain matters already goes beyond situations where there is a contractual obligation between the parties. In addition, AFCA's fairness jurisdiction should also inform the approach, so that consumers can access justice, and seek redress and protections where a receiving ADI is clearly failing to meet its obligations to retrieve funds under the Code.

**Jane's story**

Jane is a 72-year-old woman living in Perth. She had mistakenly transferred two lots of $5,000 over two days from her account with Bank A to an incorrect account with Bank B. Jane thought this Bank B account was her son's bank account.

A week later, her son called Jane to let her know he had not received the money. Jane realised that the account numbers were incorrect. Jane called Bank A to inform them of the two mistaken internet payments.

Bank A reported the two Mistaken Internet Payments to Bank B.
Approximately one month later, one lot of $5,000 was returned to Jane's account. Jane went to a local branch for Bank A and was told that the inquiry had been closed.

Jane reactivated the inquiry, but later received a letter stating that Bank B declined their request to recover the mistaken payment for the second $5,000.

Bank A had tried to contact Bank B but received no response. Jane receives a fortnightly pension, and the loss of $5,000 had a significant impact on her finances.

Jane then contacted CCLSWA. Acting on advice given on our telephone advice line, Jane made a complaint to Bank A's Internal Dispute Resolution department. Bank A told Jane they had contacted Bank B twice about the transaction, and Bank B stated they received no response from the recipient or that the recipient was not returning the money.

CCLSWA then opened a case file and assisted Jane in taking the matter to the ombudsman on the basis that Bank B failed to use reasonable endeavours to trace the money and refund it to Bank A and Jane, contrary to the e-Payments Code.

As a result of CCLSWA assisting Jane to bring a dispute, the second payment of $5,000 was retrieved for Jane.

As Jane was not an account holder of Bank B, Jane had little recourse to complain about their conduct other than through her Bank A (which she was reluctant to do, as she thought her bank had been very helpful trying to recover the funds).

Jane was particularly upset however, about her treatment by Bank B, which included a representative from Bank B calling her directly (despite CCLSWA being her legal representative at this time) to admonish Jane for her carelessness in entering the wrong online banking account number.

3.55 CCLSWA considers ASIC should extend the Code to allow for consumers to be able to complain about the conduct of receiving ADIs who have not complied with the Code, and amend the AFCA Rules to allow AFCA to make determinations against a receiving ADI regarding MIP disputes.

3.56 This amendment to the AFCA Rules is important, as it would allow our clients, such as Jane, to bring a dispute against the party that has failed to meet its obligations, rather than the bank that she feels has treated her well and with which she wants to preserve a good relationship.

3.57 We also propose that AFCA be allowed to apportion liability in circumstances where a complaint is made, and the receiving ADI has been found to have failed to comply with its obligations under the Code.

3.58 We refer ASIC to the approach taken in the United Kingdom, where the "*Contingent Reimbursement Model Code for Authorized Push Payment Scams*" (the **UK Code**)[3] has provisions for apportionment of liability to compensate customers for losses resulting from an authorised push payment scam where the sending and receiving banks have failed to meet the standards set out in the UK Code.

## Definition of 'mistaken internet payment'

C3Q1 Do you support our proposed clarification of the definition of 'mistaken internet payment'? If not, why not?

C3Q2 Please compare the costs and regulatory benefit of the following alternative scenarios:

a) 'Mistaken Internet Payment' is defined to refer only to actual mistakes inputting account identifier
b) 'Mistaken Internet Payment' is defined to include situations where a consumer inputs the incorrect account identifier as a result of falling victim to a scam (also known as 'authorised push payment fraud').

[3] See https://www.lendingstandardsboard.org.uk/crm-code/

3.59 CCLSWA does not support this "clarification" at C3 to remove scams from the definition of MIP.

3.60 While we are encouraged by ASIC's intention to engage with stakeholders on how to best tackle scams, we consider it would be premature to remove scams from the definition of MIP in the Code in advance of that consultation. Until consumers have an appropriate alternative to seek redress due to loss caused by scams, then the Code should allow consumers to make a claim for return of funds lost to scams, including authorised push payment scams, under the MIP framework.

3.61 In relation to cost, as stated above, we cannot comment on the costs to industry, but we emphasize the enormous cost to consumers, and the wider community including small business owners, from being a victim of MIP scams.

3.62 There have been reports of an increase in authorised push payment and business e-mail compromise fraud in Australia over recent years. In 2019, business email compromise fraud caused the highest losses amongst fraud losses.[4]

3.63 CCLSWA is antidotally aware of the costs to small business as we are on occasion contacted by small business owners seeking assistance on how to seek redress for emailed invoice-fraud related scams. However, as the scope of our service does not extend to small businesses, we refer such callers to other community based legal services.

3.64 CCLSWA advocates for ASIC to include authorised push payments and transfers that have been made as the result of a scam in the definition of 'Mistaken Internet Payment', in the absence of other protections at this time.

3.65 We are comforted by ASIC's recognition of scams as a problem at paragraph 64 of CP 341: "*we accept that scams are a significant and increasing problem. Therefore, we intend to work with stakeholders to contribute to addressing the problem as best we can through mechanisms other than the Code*."

3.66 As mentioned previously, banks in the United Kingdom are members of a voluntary code to deal with authorised push payment scams under the UK Code. The UK Code places obligations on member banks to identify customers who are vulnerable and provides that consumers should be reimbursed for their losses from the authorised push payment scams, in certain circumstances. We consider that Australian consumers would greatly benefit from a similar approach to the UK Code. ACCC data shows that these kinds of payment redirection or invoice scams are on the rise. [5]

[4] See https://www.scamwatch.gov.au/news-alerts/business-email-compromise-scams-cost-australians-132-million

[5] See https://www.accc.gov.au/media-release/payment-redirection-scams-cost-australian-businesses-14-million

3.67 Given the prevalence and the extent of the problems that scams cause, we consider it contradictory to ASIC's declared intention to ensure the Code's continued relevance and effectiveness, that ASIC seek to remove this important protection for consumers when currently there exists no other code, legislation or guideline that would replace these protections.

3.68 The harsh reality is that Australian consumers are losing money daily to scammers. We encourage ASIC to look to the UK Code as an example of an approach that addresses consumer vulnerability. In the interim, however, ASIC must maintain the Code's current protections, as otherwise consumers who are victims of certain scams will be left with little to no options to recover lost funds.

## On-screen consumer warning

| |
|---|
| C4Q1 Do you support our proposals? If not, why not?<br><br>C4Q2 Should precise wording for the on-screen warning be prescribed, or should flexibility as to the precise wording be allowed? If precise wording is prescribed, what should that wording be? If the Code allows flexibility, what wording would serve as a useful benchmark for compliance with the on-screen warning requirement? |

3.69 CCLSWA supports the proposed requirement to provide additional information in the on-screen warming about MIPs.

3.70 However, we would emphasise that this is an additional requirement and the provision of a warning and information about MIPs and the possibility of a consumer not being able to recover funds does not diminish the subscriber's responsibility to investigate and report a MIP.

3.71 Further any warning should not have the effect of limiting the subscriber's liability. Effective warning should be understandable, clear, impactful, timely and specific.

3.72 We believe that the wording for any on-screen warning should be prescribed, in a similar vein to the requirements for warnings in relation to Small Amount Credit Contracts prescribed in the National Consumer Credit Protection Regulations 2010.

3.73 The prescribed warning should be in plain language, clear, have the necessary impact and severity and be given at an appropriate time.

| C4Q3 What costs and regulatory burdens would be involved in implement the proposed change? |
|---|

3.74 We consider that subscribers are in the practice of providing warnings to consumers, and constantly monitoring and updating their online banking systems.

3.75 We cannot comment on the specific costs to industry in implementing this change to on-screen warnings, but CCLSWA considers that the likely reduction in consumer losses to scams (that industry may otherwise ultimately bear) would outweigh any cost to industry in implementing the proposed change.

3.76 Further, providing prescribed wording from ASIC would likely reduce the cost for subscribers in having to formulate their own wording to comply with any set "minimum requirements".

3.77 We note that ASIC has strongly encouraged subscribers to monitor the incidence of MIPs after they revise their warning message as a result to changes to the Code. ASIC may wish to make such reporting mandatory, to give ASIC the required data to assess the efficacy of the on-screen warning.

# 4 Part E: Clarifying the unauthorised transactions provisions

| E1Q1 Do you agree with our proposals? If not, why not? |
|---|

## Reducing protections for scam victims

4.1 We disagree with ASIC's proposal at E1 to "clarify" the unauthorised transaction provisions under the Code to not apply to consumers who are victims of scams where the consumer has performed the transaction themselves, within the context of a scam or misunderstanding.

4.2 Similar to our view regarding ASIC's proposal to remove scams from the definition of MIP at C3, we have deep concerns regarding the proposal at E1 removing vital consumer protections from the Code in the absence of any alternative regulatory recourse for the victims of scams.

4.3 CCLSWA has seen a recent increase in callers who have been the victims of various telephone and online banking and remote access scams, particularly where the consumer is tricked into disclosing a pass code, transferring funds to a scammer's account, or allowing a scammer to remotely access their online banking, without their knowledge.

4.4 Such scammers usually trick victims, by posing as a trusted person from a reputable company or organisation. In Charlie's situation, detailed below, he was conned by the offer of a refund relating to his slow internet speed complaint. These scams are highly

sophisticated, as Charlie had genuinely experienced poor internet connection and previously complained about his internet service provider.

**Charlie's story**

Charlie is a middle-aged man living in suburban Perth. He was contacted in March 2021 by someone claiming to be from the National Broadband Network (NBN). They told Charlie that his internet provider could not deliver the promised speed because of a problem with the NBN. Charlie was transferred to another person pretending to be from the internet provider's technical department. Charlie was told that they needed a lower package and further tests needed to be done to see what was affecting the speed. Charlie gave access to the internet provider to place a CPU status tracker on his computer, which ran in the background. The internet speed started to increase, which Charlie found promising.

The scammer pretending to be Charlie's internet provider then offered him a refund of $150 as a gesture of goodwill, as Charlie had apparently been paying too much for a service which was not being provided. The scammer asked Charlie to log into his internet banking to facilitate the transfer, which Charlie did.

The scammer told Charlie that they had accidentally put in a refund of $15,000 instead of the $150 agreed. The scammer showed Charlie an extract from their account on the screen, which showed the $15,000 entry. The caller said they needed to reverse the charge quickly or they would be fired. So Charlie authorised the purported internet provider to correct the "error". Charlie then lost access to his online banking.

Charlie contacted his bank who informed Charlie that there was some unusual activity on the account. Charlie was blocked from his online banking. Charlie then decided to contact their internet provider using their generic number to check what was going on. The genuine internet provider company had no records of the conversation about his account.

At this point Charlie realised that he had been scammed. The scammer had transferred almost $20,000 to a bank account with another bank. Charlie usually would get a verification code or challenge question when making such transfers, but he thinks that hadn't happened. Charlie called his bank to explain what had happened. The bank said that they could only recover $60 from the receiving bank.

Later Charlie was offered compensation on the condition that there would be no further investigation.

4.5 As ASIC is aware, scams are an increasing threat to consumers in Australia, and certain sections of the community such as older people, are particularly vulnerable to online and telephone-based scams. Due to the COVID-19 pandemic, Australian consumers have generally been more vulnerable to online scams as more time is spent at home on the internet. According to ACCC data in 2020, Australians lost a reported $175 million to scams compared to $142 million in 2019. ACCC data also shows that reports in 2020 increased to 216,086 from 167,801 in 2019[6].

[6] See: https://www.scamwatch.gov.au/scam-statistics

4.6 Without an appropriate alternative framework to deal with funds lost as a result of scams, CCLSWA does not think it is appropriate to exclude certain scams or mistaken transfers from the definition of unauthorised transactions in the Code as proposed in E1(a), or amend the pass code security requirements in E1(b) to prohibit disclosure to *anyone* (subject to exemptions in clause 12.8 and 12.9 of the Code).

4.7 The Code in its current format, while not a perfect instrument, establishes a process for dealing with unauthorised transactions, that does provide certain protections to consumers who are scammed. We maintain that the current Code's definition of unauthorised transactions should not be changed before any alternative protections are brought into force to provide improved levels of protections for consumers.

4.8 CCLSWA witnesses, both through our clients and our education programs, that there is a perceived degree of shame and consumer culpability in the community when talking about scams, particularly if a person has been tricked into giving a pass code or transferring funds to a scammer. However, not all consumers can be expected to protect themselves from scams, particularly where a consumer is vulnerable due to age, disability, language, illiteracy, or other such factors.

4.9 We hear stories of highly sophisticated scammers, who gain trust and confidence of our clients. So even sophisticated consumers can be easily duped[7]. It can be easy in hindsight, away from the situation, to know that a scam has been perpetrated, but at the time, our clients who are victims of scams truly believed that they were providing information or payments to genuine third parties.

4.10 John's story below, is a common example of how scammers frequently target older people who may be less technologically savvy, and more susceptible to online remote access scams that prompt them to involuntarily disclose a pass code.

**John's story**

John contacted CCLSWA in early 2021 after falling victim to an online scam. John is an elderly man, who lives by himself in the outer suburbs of Perth and he is on the aged pension.

In late 2020, John was having difficulty setting up Microsoft Windows on his newly purchased computer. John saw a pop-up message appear on his computer screen telling him that his computer had a problem, and that he should call the phone number being displayed on his screen to talk to a Microsoft technician.

John called the number and spoke to a man who identified himself as a Microsoft employee, who gave various details to satisfy John it was a genuine call. The scammer tricked John into downloading software which gave the scammer remote access to John's computer. The screen went blank, effectively locking John out of his computer without him knowing his

[7] See: https://www.abc.net.au/news/2021-06-24/inside-the-australian-bonds-investment-scam/100120448

computer was being accessed. The scammer was able to log into John's internet banking portal, but John had no idea this was happening.

John received a text message from his bank and the scammer asked John for the code in the message. After hours on the phone with the caller, John trusted the scammer, and genuinely believed he was trying to help him fix his computer, so he provided the code over the phone after the scammer said it was for a test. This allowed the scammer to transfer almost $20,000 out of John's bank account.

The scammer still had control of John's computer and the screen was blacked out for a few days. The next morning, a different person called John's mobile phone claiming to be another Microsoft employee. Again, John provided the text message code as he believed it was for a test to fix his computer. Later that day, John realised he had been scammed as another $2,000 was transferred.

John was deeply distressed about losing so much money, being a year's worth of income as a pensioner. He spoke to his bank but they told him there was nothing they could do, as no funds were able to be recovered.

The bank said that John was liable for the loss because John gave the scammers the pass codes, and this was in breach of the terms and conditions of his account.

CCLSWA lodged a complaint on John's behalf with his bank, and then escalated the matter to AFCA, on the basis that any disclosure of John's pass code to the scammers was involuntary, and the bank must show that John was more than 50% responsible for the loss.

4.11 We disagree with ASIC's proposal at E1(b) to reword the pass code security requirements, to prohibit disclosure to "*anyone*". CCLSWA are concerned that vulnerable clients such as John would no longer receive protections where they are tricked into giving a pass code to a scammer on an involuntary basis.

4.12 Under the existing Code provisions at clause 12.2(a), we consider John's disclosure should not breach the pass code security provisions of the Code because it was not "voluntary". John admitted he disclosed his pass code to the scammer for the "test" – yet we consider this disclosure was not "voluntary", given the pressure tactics and sophistication of the scammers, combined with our client's old age and limited ability with technology, this disclosure was unwitting.

4.13 We consider that banks must play a crucial role in protecting their account holders from the predatory behaviour of scammers, who are highly sophisticated. We again refer ASIC to the UK Code and encourage its consumer-friendly approach to apportioning liability in authorised push payment scams.

4.14 Under the UK Code, banks are required to assess a consumer's vulnerability (which is broadly defined) and must reimburse the consumer for their loss, unless certain exemptions apply

(such as gross negligence, or the consumer acted dishonestly or obstructively in a material respect).[8]

4.15 CCLSWA also supports AFCA's approach in its determinations which view the Code in a manner to afford a consumer the most protection.[9] Banks benefit hugely from the transition to electronic banking systems, whereas older consumers who would otherwise attend a local branch in person for their banking purposes, are now exposed and vulnerable targets for scammers.

4.16 In John's case above, the bank did not address its obligations under the Code when John raised a complaint, but instead the bank relied on its own security provisions in the terms and conditions for John's bank account. This demonstrates the lack of understanding that many banking staff have of the Code and its operation and we reiterate our position at para 3.6 – 3.7 above.

4.17 While vulnerability is a significant factor in the clients contacting us for advice, there are also circumstances where even consumers who are technologically savvy experienced in online payments can still fall victim to scams.

4.18 Lucy's story below is illustrative of how scammers are increasingly using new technologies, and prey on people's fear of being defrauded, to gain trust and access to people's pass codes, and anyone can fall for such scams.

**Lucy's story**

Lucy received a few missed phone calls from a number which appeared to be her bank's phone number. She then rang the number back but did not have time to hold. The phone call was returned and Lucy answered the phone.

The person on the phone knew personal information such as Lucy's name, address and email. They told Lucy that there was suspicious activity on her bank account, which meant they needed to cancel her cards and issue replacements. They said an SMS code needed to be sent to verify her identity. Lucy, without reading the message carefully told the person the code. Lucy is unaware as to how the scammers were able to obtain her personal information. It is believed the scammers maybe used 'number spoofing' to hijack a legitimate phone number.

After the phone call, Lucy felt uneasy and checked her account statements. She noticed a transaction for approximately $4,000 had gone through on her credit card. Lucy then reported this transaction to her bank, however due to it being a long weekend, she was not contacted until the Tuesday of the following week. Lucy filled in the disputed transaction paperwork given to her. When Lucy looked into it further, the text sent to Lucy was for a payment authorisation.

Lucy's bank attempted to do a chargeback, but it was unsuccessful. Lucy discovered that the money had been sent to a Western Union student payments portal. A person from Western

[8] See CRM-Code-LSB-Final-April-2021.pdf (lendingstandardsboard.org.uk) pages 14 and 15
[9] See, for example, AFCA Determinations 621657, and 683115: https://service02.afca.org.au/CaseFiles/FOSSIC/683115.pdf; https://service02.afca.org.au/CaseFiles/FOSSIC/621657.pdf

Union told her that the transaction was made in someone else's name. Lucy forwarded this correspondence to her bank, but they have not been helpful.

Lucy expressed concern that her bank has not been transparent or helpful during this process. Lucy's bank told her that she was liable for the amount that has been paid but offered to give her a refund of some of the funds, and not charge interest on the remaining amount. This was escalated to an internal dispute which came back with the same offer.

Lucy was not satisfied with this outcome and made a complaint to the Australian Financial Complaints Authority.

4.19 Given the level of sophistication in these scams, we strongly oppose any removal of protections while there is an absence of alternative regulatory or legislative protections for consumers. Scams are insidious and cause deep harm to people's mental health in addition to financial loss.

## Clarify that breach of pass codes contributed to the loss

4.20 We agree with ASIC's proposal at E1(d), that the Code be amended to clarify that the subscriber must prove, on the balance of probabilities, that the consumer's breach of the pass code security requirements contributed to the loss.

4.21 In CCLSWA's experience, subscribers on occasion either misinterpret the Code's provisions, or fail to apply the Code and instead rely on their own terms and conditions of the consumer's bank account (such as in John's story above) to justify refusing to accept liability for loss under the unauthorised transactions provisions.

## Chargebacks

4.22 Where an unauthorised transaction or scam occurs through a consumer's credit card there are distinct and parallel rights to raise a chargeback with the credit card provider under their credit card scheme rules.

4.23 However, there are limits to the efficacy of relying on the credit card scheme's chargeback rules in protecting Australian consumers from scams, as shown in the case studies for our clients Felicity and Bianca below.

**Felicity's story**

Felicity recently noticed a number of transactions on her account that she did not recognise. She went into her local bank branch, and they printed out a copy of her account statement and highlighted all transactions that the client did not recognise. In total Felicity identified 52 unauthorised transactions over a two-year period.

Felicity lives remotely in Western Australia and does not have reliable internet access, making it difficult to check her statements online. The transactions were all relatively small amounts – around $150. However, in total the unauthorised transactions were approximately $7,500.

The bank agreed to refund the most recent 6 transactions as they were within the 90-day reporting period for the credit card scheme. However, the bank would not refund the earlier charges totalling approximately $7,000 as they told the client that she was outside of the time limits.

4.24 Felicity's story highlights the failures of subscribers to comply with the limitation periods under the Code for unauthorised transactions where chargeback schemes may also apply.

4.25 We find that such issues particularly affect consumers living in remote areas of Australia where there is poor internet connection and where banks have encouraged paperless statements, as consumers living in remote areas are less able to frequently monitor their online bank accounts to detect any suspicious activity.

4.26 We support the proposal at E(1)(e) that ASIC clarifies liability for unauthorised transactions under the Code sits separately from arrangements available through credit card schemes. CCLSWA supports this proposed clarification to ensure that consumers such as Felicity who report an unauthorised transaction, are not prevented from redress under the Code's six-year limitation period timeframe, due to the bank's misapplication of a shorter chargeback scheme limitation period.

4.27 We also hope that this clarification will result in fewer consumers being denied the opportunity to recover funds lost to unauthorised transactions that may be linked to a credit card account, particularly for clients who are drained of their entire savings, such as in Bianca's experience, detailed below.

**Bianca's story**

In early 2021 Bianca received a text message from a person claiming to be from Amazon stating that she had bought a Dell laptop and if she did not, she should call this number back or she would be charged for the product.

Bianca called the number back and a person answered saying they were an Amazon representative. The person pretending to be an Amazon representative already had a number of Bianca's personal details including her full name, date of birth, address and credit card details and he asked her to confirm these details.

Bianca was told that Amazon would be issuing her a refund into her account. She was notified that she would receive text messages with codes and that Amazon required these numbers to process the refund.

The scammer was able to reset Bianca's internet banking password and move money from her savings account into her spending account where her credit card was linked. The scammer then proceeded to process around a dozen transactions through her credit card which amounted to around $200,000 being transferred from her bank account.

Bianca hung up the call when she noticed what was happening and immediately contacted her bank who proceeded to freeze her account with all the transactions listed as "pending".

In subsequent days the bank told Bianca that they needed to unfreeze the account because the transactions needed to process; and they unfroze the account and the money was taken.

The funds were all of her and her partner's life savings including her superannuation. Bianca had just retired due to ill health and had withdrawn all her superannuation to take advantage of government grants to build a property in which to live in rural Western Australia. Bianca and her partner have now been left with nothing and are extremely distraught.

CCLSWA are representing Bianca at AFCA in her complaint regarding unauthorised transactions under the Code, and the subscriber bank's failure to raise a chargeback. This matter is currently ongoing.

4.28 In Bianca's case, there were a number of issues relating to the bank's conduct, both with compliance with the Code's provisions on unauthorised transactions, and the availability of chargebacks given the funds were transferred through Bianca's credit card account.

4.29 We consider that cases such as Bianca's demonstrate the deep power imbalance between subscriber banks and consumers, and how subscribers fail to properly apply the Code and understand chargeback rules, to the detriment of consumers.

E1Q2 What are the costs or regulatory burden implications flowing from our proposals? Do the benefits outweigh the costs or regulatory burdens?

4.30 CCLSWA considers that any cost or regulatory burden would not outweigh the consumer detriment if ASIC removes certain scams from the Code's definition of unauthorised transactions, in the absence of other protections for victims of scams.

4.31 Without an alternative approach to protecting consumers, ASIC's proposals at E1 would leave consumers exposed to certain highly sophisticated scams without potential for redress. For clients such as Bianca, who has lost all her superannuation and savings to a sophisticated online scammer, it would be devastating to not have any legal avenue to try and get her money back.

## 5 Part F: Modernising the Code

5.1 Generally, CCLSWA supports ASIC's proposals in Part F to update and modernise the Code in line with current technology.

5.2 As a community legal centre, CCLSWA is concerned with ensuring that consumers are appropriately protected by relevant legislation and codes. If certain technology is used by consumers, such as biometric authentication, CCLSWA supports these technologies being included in the Code, rather than absent or ambiguous.

## 6 Part G: Complaints Handling

G1Q1 Do you agree with our proposals? Why or why not?

6.1 We consider that clear guidance and consistency across complaints handling provides certainty for consumers and subscribers to the Code.

6.2 CCLSWA strongly supports ASIC's proposal that all subscribers have IDR processes as set out in the new Regulatory Guide 271, and strongly supports the proposal that all subscribers be members of AFCA.

6.3 Vince's story below demonstrates the positive impact that subscribers can have when they take a proactive approach to complaints and assist vulnerable consumers to seek redress under the Code.

**Vince's story**

Vince is an elderly man living in Perth.

Vince experienced poor internet and telephone connection, and he contacted NBN regarding these connection issues. In early 2021, Vince received a call from a scammer, pretending to be an NBN technician calling him about his connection. Vince believed the call was genuine, given that he had recently contacted NBN, and Vince took steps to verify the caller's identity, including their name, contact number and job reference number.

The scammer asked Vince to perform a "speed test" on his laptop to check the internet connection levels. Vince was directed to a website by the scammer over the phone. The scammer told Vince that they would try and fix the problem, and the call ended when the scammer said something to the effect that "Telstra have gone home for the day".

The next day, the scammer called back and told Vince they were still trying to fix the issue. During that phone call, Vince received an email notification via his laptop, from his bank asking him to approve an increase to his credit limit.

Vince immediately called his bank to tell them something was wrong with his account. The bank told Vince that no transactions had been made. However, 10-15 minutes later, the bank called again to Vince's landline (while he was on his mobile phone with the scammer), to inform Vince that transactions were occurring on his account, and that Vince should immediately shut down his laptop.

Vince is sure that he did not disclose any text message codes to the scammer. Vince thinks he saw two text messages appear on his mobile to verify transactions, but the text messages are no longer available on his mobile and he thinks the scammers might have somehow wiped these.

Vince does not keep his internet banking username or password saved to his computer, and does not think he was logged in to his internet banking when the scammer was on the telephone.

Vince went to the bank and contacted the police about this scam. Approximately 9-12 transactions were made to transfer funds amounting to a loss of around $40,000. The scammers transferred $35,000 of credit from Vince's credit card account to his retirement savings account as a cash advance. The scammers also tried to apply for a new credit card in Vince's wife's name. Vince instructs that he has a daily credit limit of $5,000.

Vince complained to the bank, but he didn't get anywhere, so his adult daughter helped him complain to the Australian Financial Complaints Authority.

Once AFCA was involved, the bank properly investigated the matter and a senior manager at the bank arranged to refund Vince the entire amount of his loss from the scam, of around $40,000.

6.4 In Vince's matter, the bank refunded all of the money Vince lost to the scammers. While an excellent consumer outcome, this result only occurred after Vince's daughter lodged a dispute with AFCA about the subscriber's failures, on behalf of her elderly father.

6.5 AFCA provides a vital avenue for consumers to raise disputes under the Code when, as in Vince's experience, a subscriber initially fails to appropriately address a consumer complaint when it is first reported. It is also our experience, that in some instances, it is only after a matter has been escalated to AFCA, that the subscriber provides a sufficient response or allocates a representative with sufficient authority, such as the senior manager in Vince's case, to resolve the dispute.

| G1Q4 What would be the costs of imposing the same requirements (e.g. AFCA membership, setting up complaints frameworks, disclosure) on all subscribers? |
|---|

6.6 Whilst CLSWA cannot provide specific feedback on the costs to industry associated with requiring all subscribers to be members of AFCA and setting up appropriate complaints frameworks, we consider that the benefits to both consumers and subscribers would ultimately outweigh the costs of this requirement.

6.7 Requiring complaints frameworks, disclosures and AFCA membership provides a clear avenue for raising disputes under the Code and a clear path to escalate those disputes where required.

6.8 CCLSWA was a signatory of a joint submission to Treasury's review of the AFCA in April 2021. This submission sets out the important benefits to consumers where the other party is a member of AFCA.[10] We reiterate the view in that joint submission, that one of the most significant advances in consumer protection has been the establishment of mandatory external dispute resolution schemes such as AFCA.

6.9 CCLSWA considers that AFCA is an accessible and fair forum for people to resolve consumer banking and finance disputes. Requiring all subscribers to be members of AFCA and have a well-established complaints framework will continue that trend for positive consumer outcomes.

6.10 Bianca, John and Vince's stories reiterate the importance of being able to escalate disputes under the Code to AFCA, as otherwise consumers who have lost significant sums of money to scammers, would have little recourse if they did not receive a satisfactory outcome after raising a dispute with their subscriber bank.

[10]See: https://cclswa.org.au/joint-consumer-submission-to-the-treasurys-review-of-the-australian-financial-complaints-authority/

## 7 Part H: Facility expiry dates

| H1Q1 Do you support this proposal? Why or why not? |
|---|

7.1 CCLSWA supports ASIC's proposal to align the facility expiry period in the Code with the expiry period in the Australian Consumer Law of 36 months.

7.2 CCLSWA considers that where there is consistency across legislation, codes and guidelines the result for consumers is greater clarity about their rights and obligations, as well as more consistent and predictable outcomes in the event of any dispute.

## 8 Part I: Transition and commencement

| I1Q1 If each of ASIC's proposal in this consultation paper were to be implemented in an updated Code, what do you think an appropriate transition period would be for commencement of the updated Code? What are your reasons? |
|---|

8.1 If ASIC's proposals were to be implemented, this should be done without delay. CCLSWA supports a transition period of 6 months, as the longer the Code remains outdated and difficult to follow for consumers, the greater the risk of consumer detriment.

8.2 We reiterate that until there is a suitable alternative for consumers to recover funds lost to scams, that ASIC's proposals to remove the Code's application to scams at C3 and E1 should not be implemented.

## 9 General comments

9.1 CCLSWA consider that the Code in its current form is outdated and inaccessible for most consumers. The Code is not a consumer-facing, easily understood document. For example, the definitions and processes that apply to common consumer issues (such as a mistaken internet payment or unauthorised transaction) are difficult for consumers to grasp, and may prevent consumers from understanding, and exercising their existing rights under the Code.

9.2 We consider that the Code needs a comprehensive update to make it more consumer friendly. We can attest to the difficulty consumers have understanding the Code as we encounter difficulty and expend considerable time explaining its application to callers to our telephone advice line.

9.3 At present the Code is the main source of rights for Australian consumers to recover funds lost to scams. If, in the future, ASIC and the Government decides that scams are to be regulated under a different framework, we encourage a consumer-focused approach to

regulating liability for scams. We refer again to the UK Code which has a specific consumer information sheet which explains its rules and their effect in simple, easy to follow language. CCLSWA would encourage ASIC to adopt a similar consumer facing approach in (a) making the Code itself more comprehensible for consumers who need to rely on it to make a claim or complaint against their bank, and (b) providing a separate guide for consumers.

9.4 As referenced above, CCLSWA provides community legal education for different community groups – including to older people, who are particularly vulnerable to scams. Anecdotally speaking, when we present to these groups on scams, there is widespread acknowledgement of scams. Often when asked whether anyone has been scammed or knows of anyone who has been scammed, more than half the attendees have some experience with scams, but rarely does a person know the existence of the Code, let alone their rights under the Code.

9.5 Further we note that there is already a stigma attached to being scammed and often consumers who have been scammed are ashamed and humiliated. This stigma and shame can be the first barrier to reporting a scam and trying to recover any funds.

9.6 This barrier is only heightened when consumers attempt to access information from their bank about how they might recover any funds, and they are either given incorrect information about how the Code operates or are not even told that the Code exists.

## 10 Conclusion

10.1 CCLSWA has deep concerns about the changes proposed in CP 341 at C3 and E1. Our case studies illustrate significant consumer detriment where consumers are not able to recover funds lost to scams under provisions of the Code. The level of detriment may only be magnified by reducing the Code's applicability to scams.

We thank ASIC for the consideration of our submission and would be please to consult further on our position.

If you have any questions or would like to discuss these submissions further, please contact , Principal Solicitor on .

Yours faithfully

**Consumer Credit Legal Service (WA) Inc.**

Principal Solicitor