1st May 2019

By email: ePaymentsCode@asic.gov.au

Australian Securities and Investments Commission
GPO Box 9827
Brisbane QLD 4001

Dear Madam/Sir

Review of the ePayments Code

BACKGROUND

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.

CFA advocates in the interests of Australian consumers with and through its members, 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.

The following organisations have specifically endorsed this submission:

- Australian Privacy Foundation
- CHOICE
- Consumer Action Law Centre
- Financial Counselling Australia
- Financial Rights Legal Centre

SUMMARY

- The effective regulation of electronic payment systems, and the protection of customers using them, is critically important to Australia's consumers and to the wider economy
- Despite product innovation, banks and other businesses in this market typically have insufficient incentives to invest in and improve core systems, and issues which are at heart the result of longstanding and poor industry practices are characterised as being the fault of individual customers. This is the closest thing there is in financial services to a utility, yet the usual techniques of economic regulation as applied to infrastructure are absent.
- The objectives of the current Code are very welcome from a consumer perspective. But the wider regulatory model and the Code itself fall well short of these objectives. It should apply to all electronic payment systems, it should set out in simple terms consumers rights' and the obligations on regulated businesses, there should be effective monitoring of and reporting on both business practices and consumer experiences, there should be meaningful sanctions to create an effective deterrent for non-compliance, and it should be reviewed and updated regularly to take account of changes in technology, industry practices, consumer behaviour and the activities of third parties such as those perpetrating scams. None of these currently applies.
- The Code has some positive aspects, particularly the six objectives and the fact that ASIC has a significant role in its development and oversight. But it is hard to read and is likely to be inaccessible to many consumers (and indeed financial firms' staff). It now looks dated, not just because of developments in the industry but also because of the way in which it considers consumer behaviour.
- The most obvious solution to the issue of how to take account in the Code of the speed of change is to incorporate high-level principles, which can then be applied to a range of different technologies and businesses. Done well, this should increase rather than reduce the level of consumer protection.
- The Code has a number of gaps. It does not explicitly cover consumer vulnerability, and so is now out of line with the new version of the Code of Banking Practice. It needs to more clearly and effectively cover scams, particularly those where consumers are tricked into authorising transactions – though recent decisions of the Ombudsman in applying the Code have provided greater protection to consumers, albeit in a way that is not apparently well understood within all financial firms. There is insufficient data about compliance with the Code, and reporting requirements should not be confined to unauthorised payments. Unlike many code regimes, it includes no mechanism for consumer engagement.
- ASIC proposes a number of sensible changes, such as moving to a single complaints model.

INTRODUCTION

We are grateful for this opportunity to input to ASIC's review of the ePayments Code. The effective regulation of electronic payment systems, and the protection of customers using them, is critically important to Australia's consumers.

We have grouped our comments below in line with the topics and questions set out in the consultation paper. A summary of CFA responses is attached at Annex A.

B1: THE CODE

This review excludes issues of coverage and whether the code should be mandatory. It is worth saying, however, that we agree with ASIC's past call[1] for '*a legislative rule making power… to mandate the consumer protections in the ePayments Code. This power would allow ASIC to determine the content of the ePayments Code and monitor compliance and enforce obligations.*'

It is now more than a decade since ASIC first raised the issue of whether the EFT Code should be made mandatory[2]. More recently but still several years ago, the Financial Services inquiry[3], published in 2014, recommended that the ePayments Code should be mandatory. The following year the then Government responded[4]: '*We will ensure that minimum acceptable practices consistently apply to the payments industry in the interests of consumers. ASIC will mandate baseline consumer protections in the ePayments Code, subject to the code being fit for purpose and technologically neutral.*'

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

We are disappointed that creating a more robust ePayments regime has not been a priority for government in recent years, and we would urge the next Federal government to act as soon as possible. Consumers face real and ongoing harm because of this failure.

The Code's objectives – and the reality

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

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

These objectives are generally very welcome from a consumer perspective – though ASIC's review should consider whether they remain fit for purpose. It is for example worth considering whether the emphasis on '*effective disclosure to enable informed choice by consumers*' reflects current insight and regulatory practice in relation to consumer behaviour and information remedies.

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

[1] https://treasury.gov.au/sites/default/files/2019-03/ASIC-1.pdf
[2] https://download.asic.gov.au/media/1329878/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf
[3] http://fsi.gov.au/publications/final-report/
[4] https://treasury.gov.au/sites/default/files/2019-03/Government_response_to_FSI_2015.pdf

It should apply to all electronic payment systems, it should set out in simple terms consumers' rights and the obligations on regulated businesses, there should be effective monitoring of and reporting on both business practices and consumer experiences, there should be meaningful sanctions to create an effective deterrent for non-compliance, and it should be reviewed and updated regularly to take account of changes in technology, industry practices, consumer behaviour and the activities of third parties such as those perpetrating scams. None of these currently applies.

Our main concerns with the current voluntary regime include:

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

[5] It is however worth noting that not all Fintechs may have to be members, and while AFCA has a greatly expanded jurisdiction compared with FOS, there are still monetary limits and compensation caps in place

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

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

The accessibility of the Code

When redrafting the Electronic Funds Transfer Code of Conduct and renaming it the ePayments Code, ASIC committed to writing the Code in plain English[8]. A plain English Reference Group included a representative of Choice and CFA.

This was the right aspiration, and it remains relevant today. In our view, further drafting work needs to be done to make the current Code truly accessible to consumers.

For example, applying a series of different readability measures[9] to the text of clause 11 produces the assessment that it is 'very hard to read' and at 'college graduate' level.

Clause 12.4 states: '*A user must not act with extreme carelessness in failing to protect the security of all pass codes where extreme carelessness means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour*.' There is then an example given, which is clearer, but this text in itself is meaningless and tautological – at heart all it says is that the words 'extreme' and 'greatly' are synonyms.

CFA members report some indications that financial firms' employees may not understand the Code either, and indeed that the opacity and complexity of the language in the Code means the intent of the Code is not being delivered by subscribers.

Consumer and staff awareness and understanding of the Code could and should be tested through research.

Catering for innovation

Paragraph 25 notes that the degree of change means that the Code is unlikely to be able to anticipate developments, and so '*ASIC's role in regularly reviewing the Code will be important*.'

We agree with the need for ASIC to review the Code regularly and think the current five-year timescale is insufficient. But we would like to see more discussion of why ASIC has not been meeting its existing obligations in this market. How will ASIC ensure that it devotes necessary resources and senior management and Board attention to this area in future, and what will need to change to make sure this happens?

ASIC has previously said[10] that '*The ePayments Code contains essential consumer protections, in particular the regime for allocation of liability for unauthorised electronic payment transactions, which is not dealt with elsewhere in the law. Effective enforcement and coverage of the Code is therefore essential in promoting consumer trust and participation in electronic payments*.' But even given the limitations of the current arrangements, with the regulator having few formal enforcement powers, ASIC has apparently played a minimal role in this market over the last few years.

[8] https://www.asic.gov.au/media/1333064/cp158-published-20-May-2011.pdf
[9] We used this tool, which includes two Flesch-Kincaid measures: http://www.readabilityformulas.com/freetests/six-readability-formulas.php
[10] https://treasury.gov.au/sites/default/files/2019-03/ASIC-1.pdf

Paragraph 8 of the consultation paper notes that ASIC is required to review the Code every five years, but it last did so in a comprehensive way in 2010, nine years ago. It made a few very minor drafting amendments in 2011, 2012 and 2016. Prior to 2010, the previous Code was reviewed in 2001[11].

We acknowledge that delays over recent years were in part the result of waiting for the outcome of a series of external reviews, allied to uncertainty about the desire of the Federal government to make the Code mandatory. However, we understand that relatively few resources are devoted to this area of work within ASIC, with a very small number of staff working on it and no consumer research commissioned. We share ASIC's frustration that it has not yet been given powers to make the Code mandatory and then take enforcement action, but this is not the only mechanism available to it for driving change in the industry. It could for example commission and publish consumer research and explore the use of reputational regulation techniques, alongside the existing voluntary Code.

We would like to see this becoming much more of a priority area for ASIC, reflecting the breadth and depth of this market's impact on consumers and the potential for significant consumer detriment. If the Code remains in a form similar to now, it should be reviewed more frequently than once every five years.

The most obvious solution to the issue of how to take account in the Code of the speed of change is to incorporate high-level principles, which can then be applied to a range of different technologies and businesses. This is not a new idea. In 2008, ASIC stated[12] that '*We propose to redraft the EFT Code as a principles-based code*'. CFA supported this[13], but by 2010[14], ASIC was saying only that the Code would '*adopt a principles-based approach as far as possible'*, arguing that while all respondents to the consultation supported the use of plain English, '*There is less support, even among industry stakeholders, for a principles-based code*.' We note that since then regulators in different sectors around the world have embraced principles-based regulation more strongly, in spite of the tendency for regulated businesses to support more detailed rules. We would like to see ASIC explore this again.

These principles should so far as possible focus on consumer outcomes. For example, in relation to communication with customers, a relevant principle might be that the communication is undertaken in such a way that it can reasonably be expected to influence each customer's behaviour – not just that a message is sent to customers periodically. Or in the case of warnings sent with SMS authorisation codes, that these are sufficient to provide a meaningful alert to the customer of the dangers of sharing those codes with any person, including someone purporting to be from their bank.

This assessment by ASIC

Payments can be a complex and highly technical area, and one which requires the regulator and industry to work harder than might be the case elsewhere to ensure the consumer voice is heard and the consumer interest is put at the heart of decision-making.

[11] http://ris.pmc.gov.au/sites/default/files/posts/2011/09/03-ePayments-Code-RIS.pdf
[12] https://download.asic.gov.au/media/1329878/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf
[13] http://www.galexia.com/public/research/assets/eftreview_2008/gc328_eftreview_submission_2008_public.pdf
[14] http://download.asic.gov.au/media/1343510/rep218.pdf

The lack of consumer engagement mechanisms not just in ASIC but also the Council of Financial Regulators, the Reserve Bank's Payments Board and industry bodies, allied to little published consumer research, suggest this is not currently happening.

We would like to see:

- A regular program of consumer research, exploring customers' attitudes and experiences of ePayments systems and their awareness and knowledge of the ePayments Code. This appears to be absent at present.
- An ongoing, dedicated mechanism for engaging consumer advocates in ePayments issues. ASIC had two stakeholder working groups to support its reviews of the EFT Code from 2007 onwards. We understand that the only structured mechanism within ASIC for consumer input now is the Consumer Advisory Panel and that it has not often discussed ePayments issues. This is in stark contrast with approaches in other countries: see the case study on the UK Authorised Push Payments scams steering group.

We recognise that the latter may not be wholly easy – the nature of the issues may mean that many consumer advocates are currently not easily able to engage, and so ASIC (potentially in conjunction with the Reserve Bank's Payments Board) may need to work to build capacity in this area. Other regulators have taken steps in this respect. For example, in its Stakeholder Engagement Framework[15], the Australian Energy Regulator makes a commitment to '*Take steps where needed to build knowledge and capacity to help stakeholders to engage.*'

Case Study: Authorised Push Payment (APP) Scams Steering Group, UK

The Authorised Push Payments Scams Steering Group is led by an independent chair appointed by, and directly accountable to, the Payment Systems Regulator. In February 2019 it agreed a voluntary Code of good practice which aims to better protect customers and reduce the occurrence of APP fraud.

Members of the Steering Group are appointed by the Chair, who is a former chief executive of a consumer advocacy organisation. The Steering Group comprises an equal number of representatives of payment service providers and consumers.

Attending Steering Group meetings are observers from regulators, government and law enforcement.

Source: https://appcrmsteeringgroup.uk/governance/

[15] https://www.aer.gov.au/system/files/AER%20%20Stakeholder%20Engagement%20Framework.pdf

B2: COMPLAINTS HANDLING

The consultation paper asks whether there is justification for maintaining two complaints handling regimes in the Code. We can see no justification for retention of the current position, particularly given the flexibility provided by RG 165. There is plenty of evidence to suggest that consumers prefer and are better able to access single complaints handling regimes, and the consultation document makes a good case for change in this area.

B3: UNAUTHORISED TRANSACTIONS

The Code as currently drafted and interpreted does not adequately take account of the changing nature of scams and associated consumer behaviour. ASIC placed a reasonable degree of focus on scams in its 2007 consultation on the EFT Code[16], but it gets more limited attention here.

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

In the absence of robust published data[17], it is hard to assess precisely the prevalence of such scams, but we understand they are very substantial and growing, and action is needed now to protect consumers. In 2016, this was the subject of a 'super-complaint' by our colleagues at Which? in the UK[18], which has subsequently led to the development of significant new rules that take effect on 28 May[19]. These ensure amongst other things that where neither the bank nor the customer was at fault, the customer should be reimbursed.

One issue to consider here concerns the meaning of '*unauthorised*' and '*authorised*', and (as set out in clause 11.8(a)) '*all reasonable explanations for the transaction occurring*.' The nature of these scams is such that the consumer does literally authorise a transaction, but in doing so thinks that they are authorising a different transaction. In this respect it bears significant similarity to a mistaken payment. Indeed the Australian Payments Network describes[20] mistaken payments as including when the consumer '*had been given incorrect BSB or account details*' – the difference being that in the case of scams the incorrect account details are supplied deliberately, not in error.

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

[16] http://download.asic.gov.au/media/1337174/eft_review_2007.pdf

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

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

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

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

Case study: Clara's story

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

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

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

Source: Financial Rights Legal Centre

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

Case study: FOS decision about voluntary disclosure and extreme carelessness

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

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

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

Source: CFA summary of FOS case number 526294, 5 September 2018

https://service02.afca.org.au/CaseFiles/FOSSIC/526294.pdf

The consultation paper notes the development of scraping services and aggregators, which can require consumers to provide their passwords to a third party and so inadvertently breach the Code. As the paper notes, some of these practices are the product of other regulatory provisions. It is plainly unfair for consumers to lose protection in one area of regulation because of the application of regulation designed to protect them in another area.

CFA members report examples where staff may be unaware of the Code's provisions or may seek to take advantage of consumers' lack of knowledge – see case study below.

Case study – Rosie's story

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

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

Source: Financial Rights Legal Centre

Late last year the Australian Banking Association published its Accessibility Principles for Banking Services[21], which places emphasis on what it calls '*inclusive design*.' The Code is now out of line with this, for example in relation to protection of passwords, where a consumer might share their password with a family member or trusted friend to use services that they would otherwise be unable to access. This is considered in more detail in the ABA's Guiding Principles for Accessible Authentication[22]. It feels like there is a much more sophisticated understanding of consumer diversity, behaviour and needs in these documents than there is in the ePayments Code.

Case study: EFTPOS machine accessibility

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

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

Source: https://www.piac.asn.au/2019/01/10/a-step-in-the-right-direction-cba-to-improve-accessibility-of-albert-eftpos-machines/

[21] https://www.ausbanking.org.au/images/uploads/Accessibility_Principles_for_Banking_web.pdf
[22] https://www.ausbanking.org.au/Industry-Standards/guiding-principles-for-accessible-authentication

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

As the consultation paper indicates, there is a danger that the current rules on liability and disclosure of passwords may serve to inhibit innovation in the market, for example where fintech businesses might want to develop services allowing consumers to manage all their accounts in one place.

B4: DATA COLLECTION AND REPORTING

The Australian Prudential Regulation Authority (APRA) and ASIC have recently released a series of publications and an online tool allowing policyholders to compare life insurers' performance in handling claims and disputes[23]. The two regulators say that '*The data release signifies a new level of transparency and accountability which the regulators see as essential to improving trust in financial services.*'

This is part of a move worldwide by regulators to use 'reputational regulation' techniques – that is, to collect and publish firm-by-firm data which allows the community to see how different businesses are performing, so supporting choice and providing an incentive for businesses to improve[24].

The Productivity Commission's 2017 inquiry into data availability and use[25] found that '*Significant change is needed for Australia's open government agenda and the rights of consumers to data to catch up with achievements in competing economies*', and it called for '*a strong and clear cultural shift towards better data use.'*

In this context we are dismayed that ASIC has suspended the collection of data relating to unauthorised transactions covered by the ePayments Code, rather than considering how it can use develop a positive data strategy in this area, which might both build consumer confidence and drive performance improvements by businesses.

There is no obvious reason why the current arrangements for data reporting are limited to just one aspect of the Code, unauthorised transactions. We consider that this should be extended to cover the full Code. The absence of ASIC enforcement powers arguably makes this approach more, not less, important than in other areas of regulation.

We appreciate that ASIC may have some legal restrictions in this area and the present voluntary nature of the Code may create a reluctance to take a firm stance on data collection and publication. But we

[23] https://www.apra.gov.au/media-centre/media-releases/apra-and-asic-publish-world-leading-life-insurance-data
[24] See for example: '*The use of data publication to enable reputational regulation*', UK Regulators Network (2014) https://www.ukrn.org.uk/wp-content/uploads/2018/06/2040728-DataPubRepReg.pdf
[25] https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

would like to see ASIC adopt the energetic spirit here that it has shown in relation to life insurance company data.

More generally there needs to be significantly better data made available on ePayments, so that there can be an open dialogue between regulators, businesses, consumer groups and other stakeholders on emerging consumer harm and how best to tackle it. It is striking how little is currently published, by both regulators and industry bodies.

B5: MISTAKEN PAYMENTS

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

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

Case study: Receiving a mistaken payment

A consumer told CHOICE:

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

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

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

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

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

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

It would appear that in such cases consumers assume that because banks' own systems connect account name and numbers, this will be built into the consumer interface of electronic payment systems too. This does not feel an unreasonable expectation, and at the very least the design of warnings to customers should take account of any such perceptions – though we agree with the concerns set out in the consultation paper about the likely ineffectiveness of risk warnings in general. The most effective approach is likely to be to bring the payment system in line with customer expectations. It would appear that the PayID service which uses the New Payments Platform may represent a step forward in this respect[26], though many more customers still use BSB and account numbers and so have a service that is more open to error.

CFA members also report that they have seen many examples of blame shifting between banks: one bank says that it is the other bank that they are waiting on, and vice versa. The Code stipulates that it is the original bank's issue to address, but in practice this is not made clear to customers. Under the Code, a customer should go to the sending ADI's EDR scheme, and both ADIs must cooperate with the sending ADI's EDR scheme.

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

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

The case for 'confirmation of payee'

ASIC's counterpart in the UK has been consulting on whether banks should be required to implement a 'confirmation of payee' service, to help make sure people send their money to the intended recipient[27]. This would match the bank account number with the name of the account holder, and in doing so would both significantly reduce the number of mis-directed payments and undermine certain types of scam.

As noted above, the PayID service looks like a positive step, but not every institution has signed up to it and most customers are still using the more traditional account number and BSB service. Unless and until the PayID service becomes the standard way of sending money electronically, we think the services covered by the ePayments Code should introduce a confirmation of payee service. This would mean that consumers receive a similar degree of protection across different services.

[26] https://payid.com.au/#works
[27] https://www.fca.org.uk/insight/why-confirmation-payee-cant-come-soon-enough

While this is being implemented, we would like to see banks put in place a requirement for customers to enter payee details twice, so that typing errors can be more easily identified and quickly remedied. This is such common practice in online services nowadays that it is surprising it was not adopted long ago.

The volume of scams is increasing at an alarming rate, and according to the consultation paper 26 per cent of mistaken payments (by value) are never retrieved. This failure rate is not costed in the consultation paper, nor is the cost of making successful retrievals assessed, but we assume this must amount to many millions of dollars.

We think there is a clear business case for a 'confirmation of payee' check, which though not a negligible cost is presumably at the lower end of IT system changes, given that it involves data that businesses already hold and connect.

We encourage ASIC to explore the case for improvements in this area, and as part of this to publish its analysis of the likely costs and benefits. This should take account of take-up rates of PayID and an analysis of whether this service is indeed reducing the volume of mistaken payments.

If the industry is unwilling to engage with the case for a 'confirmation of payee' system, we consider that a future mandatory version of the ePayments Code should require businesses to bear the full cost of all genuine mistaken payments, so that consumers do not lose out as a result of any industry under-investment.

The Ombudsman has accepted precisely this argument – see the case study below. However, this case also shows the weakness of the Code. In order to reach this decision to protect the consumer, the Ombudsman had to conclude that the ePayments Code did not apply to this case. If it had applied, the consumer would apparently have been left unprotected.

Case study: FOS decision on confirmation of payee

The customer was the intended recipient of a $10,000 payment from a real estate agency. The applicant gave the agency an incorrect account number, but the correct account name and BSB. The payment was made into an unintended third party's account, who withdrew the funds a day later and did not respond to several requests return the funds.

FOS determined that the financial firm should pay the money to the customer, as owes its customers a duty of due care and skill when receiving funds on their behalf. FOS said: '*It is a commercial decision for the FSP to have a system which does not allow the account name to be checked when it is receiving funds on its customers behalf. However, it then accepts the risk that it is liable to reimburse the applicant for the payment when it has not complied with its obligations to her as the intended recipient*.' The ePayments Code did not apply, as the customer was the recipient not the sender and the payment came from a business account.

Source: CFA summary of FOS Case number 526105, 18 September 2018
https://service02.afca.org.au/CaseFiles/FOSSIC/526105.pdf

In other cases, the Ombudsman has given a degree of protection to the consumer in relation to mistaken payments, including involving scams. In one recent case[28], the consumer needed to pay his builder over $85,000, and his email was hacked and the account details changed in the builder's invoice, so the money was paid to a scammer. The Ombudsman decided this should have been treated as a mistaken payment under the Code. In another recent case[29], the customer wanted to make a payment overseas worth $62,000 and provided transfer instructions to his bank. The beneficiary bank named in the transfer form did not exist and did not match the SWIFT code provided. The Ombudsman decided that, in the circumstances, the bank should have made further enquiries with the complainant to confirm the transfer details provided were correct before making the transfer. The bank was told to pay the complainant 50% of the transfer.

These decisions, while welcome, indicate the complexity of applying the Code to individual cases, and the need for more clarity in the Code allied to better understanding within financial firms about its meaning.

B6: SMALL BUSINESSES

CFA does not represent small businesses as consumers and so these questions are beyond our remit.

B7: GAPS IN THE CODE

Consumer vulnerability

The new version of the Code of Banking Practice[30], which takes effect on 1 July 2019, says that '*We will take extra care with vulnerable customers*', and Part 4 of that Code more generally makes a series of

[28] Case number: 523124. https://service02.afca.org.au/CaseFiles/FOSSIC/523124.pdf
[29] Case number: 526951. https://service02.afca.org.au/CaseFiles/FOSSIC/526951.pdf
[30] https://www.ausbanking.org.au/images/uploads/Banking_Code_of_Practice_2019_web.pdf

commitments relating to inclusive and accessible banking. A new industry guideline on supporting vulnerable customers is being developed alongside this[31]. The lack of anything about consumers in vulnerable situations is a major gap in the ePayments Code – not least as older customers tend to be disproportionately represented in scam losses.

Scams

As noted above, the Code needs to more clearly and effectively cover scams, particularly those where consumers are tricked into authorising transactions.

Reporting

As noted above, there is insufficient data about compliance with the Code, and reporting requirements should not be confined to unauthorised payments.

Consumer engagement and insight

Many self-regulatory code regimes have mechanisms for consumer engagement, to offset the role of the relevant industry in establishing and running the regime. Paradoxically the role of ASIC in relation to the ePayments Code may mean this was not perceived to be necessary, and so there is less consumer engagement here than in relation to other codes. This needs to be remedied.

[31] https://www.ausbanking.org.au/media/media-releases/media-release-2019/raising-the-bar-to-help-customers-doing-it-tough

Annex A: ASIC questions – summary of CFA views

ASIC areas of focus	ASIC questions	CFA view
B1 We propose to assess whether the Code, as currently worded, has successfully adapted to today's payments environment and is sufficiently adaptable to respond to emerging and future developments in financial technological innovation and changing customer behaviours.	B1Q1 Are you aware of any specific examples where the Code is not adequately catering for these things?	The voluntary nature of the Code is a significant issue for consumers which needs to be resolved. ASIC needs to develop its understanding of consumer harm in relation to ePayments and set out its strategy to tackle this, then use the Code as one tool to achieve its desired objectives. Updating with the Code without having a robust, evidenced, well-considered and suitably-resourced approach underpinning it will not be effective.
	B1Q2 How could our assessment of these things be done in a simple and consumer-focused way?	ASIC should start by considering whether the Code's objectives are the right ones and are met through the current arrangements. The issues here are not simple and there is unlikely to be a wholly simple approach to tackling them. We welcome the commitment to working in a consumer-focused way, but this needs to extend significantly further than the Code alone. We propose that ASIC establishes mechanisms for consumer and wider stakeholder engagement, as it did a decade ago.
B2 We propose to assess the clarity and appropriateness of the current policy positions in the Code's complaints handling provisions.	B2Q1 Is there justification for maintaining two complaints handling regimes in the Code (i.e. Chapter F and Appendix A)?	No. There is plenty of evidence to suggest that consumers prefer and are better able to access single complaints handling regimes, and the consultation document makes

		a good case for change in this area.
	B2Q2 Would there be any benefits in more closely aligning the complaints handling provisions in the Code with RG 165?	Yes. This should improve consumer access and outcomes.
B3 We propose to consider whether the current settings in the Code for unauthorised transactions are appropriate and sufficiently clear	B3Q1 What are the benefits and challenges of the Code's current settings for unauthorised transactions?	Some practices which appear to breach the Code's provisions on protection of passwords are the product of other regulatory provisions. It is plainly unfair for consumers to lose protection in one area of regulation because of the application of regulation designed to protect them in another area. There is also a danger that the current rules on liability and disclosure of passwords might serve to inhibit innovation in the market, such as services where consumers can manage all their accounts in one place.
	B3Q2 What role, if any, could the Code play in preventing or reducing the risk of customers falling victim to financial scams, or helping customers who have lost money through scams?	The Code as currently drafted does not adequately take account of the changing nature of scams and associated consumer behaviour. We are particularly concerned about scams where the consumer is tricked into authorising a payment to an account that they believe belongs to a legitimate payee but is in fact controlled by a scammer. The Code's silence on this is at odds with emerging best practice in other countries. Recent Ombudsman decisions offer greater protection to consumers, but it is apparent that these decisions have not

		been fully understood and embedded by all financial firms.
B4 We propose to review the data reporting requirements in the Code and assess the most valuable and efficient approach	B4Q1 Would it be helpful (for consumers or subscribers or both) for ASIC to collect and publish data about particular matters under the Code? If so, what matters, and why?	We strongly support the collection and publication of both industry-wide and firm-by-firm data, to build consumer confidence and drive improvements in business performance. This should extend beyond unauthorised payments.
B5 We propose to consider whether the provisions in the Code for mistaken payments are simple and accessible enough, and whether ADI subscribers should have any role in mitigating or preventing such payments.	B5Q1 Is the process for seeking return of mistaken internet payments sufficiently simple for customers?	The primary focus should be on preventing mistaken payments through improvements in the design of systems, not just on trying to get money back once it is lost. The rules on mistaken payments should include payment of the wrong amount as well as to the wrong account.
	B5Q2 What other provisions could be included in the Code for ADI subscribers to reduce the risk of or prevent mistaken payments?	We would like to see the industry introducing a requirement to type account details twice, and then the implementation of 'confirmation of payee', in which account details and the name of the accountholder are matched.
	B5Q3 To what extent do you think the mistaken payments procedures in the Code will remain relevant as more customers begin using the New Payments Platform?	As payments systems become faster, it will be ever more important to minimise mistaken payments through good system design, rather than relying on moves to get the money back afterwards.
B6 We propose to explore whether it may be appropriate to extend the Code, or at least	B6Q1 Do you think that all or any parts of the Code should, or could appropriately, apply to small business?	CFA does not represent small businesses as consumers and so these questions are beyond our remit.

some of its protections, to small business.	B6Q2 Are you aware of any data that shows the prevalence of electronic banking problems for small business customers? B6Q3 How might the Code best define 'small business'?	
B7 We propose to consider any other aspects of the Code that may need updating as part of our review.	B7Q1 Are there any other aspects of the Code that should be updated?	The most obvious failing of the Code remains its voluntary nature. It should incorporate some high-level principles, so making it more adaptable to emerging services. ASIC should be required to review it more frequently than once every five years, and should demonstrate how it will ensure this actually happens. The Code has a number of gaps. It does not explicitly cover consumer vulnerability – and so is now out of line with the new version of the Code of Banking Practice. It needs to more clearly and effectively cover scams, particularly those where consumers are tricked into authorising transactions. There is insufficient data about compliance with the Code, and reporting requirements should not be confined to unauthorised payments. Unlike many code regimes, it includes no mechanism for consumer engagement.