**Westpac Group Response - ASIC Consultation Paper 342: Review of the ePayments Code**

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| **B1** | **Compliance and Industry Monitoring** | | |
| | We propose to do the following:<br>(a) remove the requirement in clause 44.1 of the Code that subscribers must report annually to ASIC or its agent information about unauthorised transactions; and<br>(b) retain ASIC's power to undertake ad hoc targeted compliance monitoring (presently in clause 44.2), but specify two distinct functions:<br>(i) monitoring subscribers' compliance with Code obligations (which already exists in clause 44.2); and<br>(ii) monitoring or surveying matters relevant to subscribers' activities relating to electronic payments. | **B1Q1** Do you support removal of the requirement in clause 44.1? If not, why not?<br><br>**B1Q2** What are the costs to subscribers of ASIC continuing an annual collection of data on unauthorised transactions? How does this compare to the potential costs and benefits or savings of ASIC instead relying on its ad hoc monitoring power in the Code?<br><br>**B1Q3** Do you see any possibility for industry-led recurrent data collection and reporting in relation to unauthorised transactions? What would be the costs of setting up and maintaining such an initiative, and who would be well placed to conduct it? | **B1Q1 & Q2**<br>We support the proposal to remove the annual reporting requirement in clause 44.1 of the Code and note that the annual collection of data for unauthorised transactions has been on an extended pause for a number of years. We believe that the proposal for ASIC to retain power to undertake ad-hoc targeted compliance monitoring (as in clause 44.2 of the Code) is sufficient.<br><br>As the annual collection has remained on hold since 2018, there is currently no cost associated with this. To re-establish annual reporting, the cost would not be insignificant, as we have changed a number of systems since the last report. We can typically accommodate ad-hoc reporting with nominal cost.<br><br>**B1Q3**<br>There are existing bodies that facilitate similar functions to that outlined in B1Q3. The Australian Financial Crimes Exchange (AFCX) currently facilitates the listing of all key transactional frauds for the purpose of collating losses, but also for extracting and sharing relevant intelligence, such as destination accounts of unauthorised transactions.<br><br>The AFCX data-share was established in response to ASIC's initial reporting requirements and has been in place for over two years. The data is currently shared intra-day, where the shared intelligence feature is an incentive for submissions. Currently only a select number of Code subscribers are also members of the AFCX. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | **B1Q4** Do you support the additional monitoring or surveying function in proposal B1(b)(ii)? If not, why not?<br><br>**B1Q5** What are the expected costs to subscribers of the additional monitoring or surveying function mentioned in proposal B1(b)(ii)? | Additionally, submissions are provided to AusPayNet for annual reporting (for cards, cheques, and digital transactions) that collate and report card fraud data.<br><br>Further investigation would be necessary to identify the costs, any regulatory burden and to determine the onus of establishing an '*industry-led recurrent data collection and reporting'* body or augmentation of the AFCX. We would welcome industry discussion on this.<br><br>**B1Q4 & Q5**<br>We are supportive of the additional monitoring or surveying function mentioned in proposal B1(b)(ii). However, for us to fully assess the proposal, and any associated costs, we welcome further clarification and specificity with regard to the type of monitoring or surveying, and the scope and frequency of such monitoring and surveying. |
| **C1** | **Partial return of funds** | | |
| | We propose to amend the Code so that:<br>(a) the processes in clauses 28, 29 and 30 apply not only where there<br>are sufficient credit funds available in the recipient's account to cover the mistaken internet payment (current application) but also where only a portion of the funds is available in the recipient's | **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?<br><br>**C1Q2** Are there benefits in applying the MIP framework to situations where only partial funds are available for return? Please describe these benefits. | **C1Q1 & Q2**<br>Our view is that there are no 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.<br><br>In our view, as the main purpose is to limit consumer loss, returning a partial payment through any available funds in a recipient's account fits well with the intention of the Code and may also result in a reduction in complaint volumes.<br><br>**C1Q3-Q7**<br>It would be very helpful for non-exhaustive examples to be provided as the term '*reasonable endeavours'*, with respect to actions taken pursuant to the Code, is very broad. Furthermore, subscribers, third parties and other regulators or bodies |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | account (so that the consumer has an opportunity to retrieve at least a portion of the mistaken internet payment);<br>(b) it includes non-exhaustive examples of what a receiving ADI can do to meet the requirement to make 'reasonable endeavours' to retrieve the consumer's funds, while clarifying that these examples are guidance only and are neither a 'safe harbour' nor prescribed actions that the receiving ADI must in every case take; and<br>(c) proposals C2(a) and (b) operate together—that is, the receiving ADI must seek return of the partial (if any) funds and make reasonable endeavours to retrieve the remainder of the funds. | **C1Q3** Do you think it would be useful for the Code to provide non exhaustive examples of what might amount to 'reasonable endeavours'? If not, why not? | may have varying subjective interpretations, which may result in actions taken by subscribers being inconsistent. This may cause poor consumer outcomes and increased costs and regulatory burden upon the subscriber.<br><br>Clarifying expectations on the receiving ADI would be beneficial, for example, such as:<br>• the receiving ADI should send correspondence to the unintended recipient via their preferred channel (email, mail);<br>• in the case of no response from the unintended recipient, the receiving ADI should follow up with one additional follow-up correspondence;<br>• where there are insufficient funds held in the destination account or the account is closed, but sufficient funds are in other accounts owned by the same account holder, the receiving ADI should debit those funds in satisfaction of the MIP.<br><br>Clause 32.1 of the Code provides an example as to what may constitute reasonable efforts and we would welcome similar guidance where the term *'reasonable endeavours'* is used throughout the Code. Factors affecting whether a particular action is necessary to satisfy reasonable endeavours include:<br>• responsiveness of the unintended recipient to contacts by the receiving ADI; and<br>• status of the account into which the funds were deposited (e.g. closed).<br><br>The practicality and costs of implementing the proposals at C1 depends upon what constitutes *'reasonable endeavours'* and the non-exhaustive examples given as guidance, as these may be significant. However, simply returning partial funds does not present significant practical impediments. |
| | | **C1Q4** What types of examples would be helpful in a non exhaustive list of examples of what might amount to 'reasonable endeavours'? | |
| | | **C1Q5** What types of factors might affect whether a particular action is necessary to satisfy 'reasonable endeavours' in individual cases? | |
| | | **C1Q6** Are there any practical impediments to implementation of the proposals at C2? | |
| | | **C1Q7** What are the costs to subscribers of extending the MIP framework to cover the partial return of funds? | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| **C2** | **Responsibilities of the sending and receiving ADIs** | | |
| | **We propose to amend the Code to: (a) require the sending ADI to investigate whether there was a mistaken internet payment and send the request for return of funds to the receiving ADI 'as soon as practicable' and, in any case, no later than five business days after the report of the mistaken internet payment;**<br>**(b) require both the sending and receiving ADIs to keep reasonable records of the steps they took and what they considered in their investigations;**<br>**(c) require the sending ADI, when they tell the consumer the outcome of the investigation into the reported mistaken internet payment, to** | C2Q1 Do you agree with the proposed timeframe in proposal C2(a)? If not, why not? | **C2Q1 & Q2**<br>We agree with the proposed timeframe in proposal C2(a) and note that this is our current practice. There would be no additional costs associated with compliance with the proposed timeframe. |
| | | C2Q2 What are the costs associated with compliance with the proposed timeframe? | **C2Q3**<br>We agree with the proposed record keeping requirements. Whilst we currently retain records, we would need to modify our current standard to incorporate any new or additional requirements implemented by the Code. We would welcome examples of what ASIC considers 'reasonable records' as these would be helpful. |
| | | C2Q3 Do you agree with the proposed recording keeping requirements? Why or why not? What are the costs of the proposed record keeping requirements? | **C2Q4**<br>The costs of requiring the ADI to advise the consumer of their rights to complain would be limited to the costs of drafting and implementing updated collateral, which we do not expect to be substantial. |
| | | C2Q4 What do you consider are the costs of requiring ADIs to inform consumers of their dispute resolution rights? | **C2Q5**<br>Proposal C2(d) would potentially carry an increased burden on the sending ADI. Non-cooperation by the receiving ADI or the unintended recipient may present the need for the sending ADI to take additional steps for their actions to be considered *'reasonable endeavours'*, rather than merely following the process as laid out in the |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | **include details of the consumer's right to: (i) complain to the sending ADI about how the report about the mistaken internet payment was dealt with; and (ii) complain to AFCA if they are not satisfied with the result; and (d) clarify that non-cooperation by the receiving ADI or the unintended recipient is, by itself, not a relevant consideration in assessing whether the sending ADI has complied with its obligations.** | 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? | code. Ideally, in order to provide further clarity, ASIC's expectations in such a situation would be welcome, as per our response to C1Q3-Q7. |
| **C3** | **Definition of 'mistaken internet payment'** | | |
| | We propose to amend the Code to clarify the definition of 'mistaken internet payment' to ensure that it only covers actual mistakes inputting the account identifier and does not extend to payments made as a result of scams. | **C3Q1** Do you support our proposed clarification of the definition of 'mistaken internet payment'? If not, why not? | **C3Q1** We support the proposal to clarify the definition of 'mistaken internet payment' (MIP) to not include payments made as a result of scams, as this will provide a clearer pathway for consumers. MIPs are genuine mistakes made by consumers where they have input details incorrectly. Such payments should therefore follow the MIP process.<br><br>In our view scams should be excluded from the definition of MIP. Additionally, the Code should make clear the distinction. For example, if authorised push payments scams (most notably Business Email Compromises) were considered as 'mistakes', this in our view, would immediately cloud this distinction and does not capture the spirit of a 'mistake' as purely an input error. We propose that the Code guide |
| | | **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 the account identifier. | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | (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'). | subscribers on how to distinguish a push payment scam from a MIP, as this would facilitate optimum consumer outcomes.<br><br>Further to this, the protocol for MIPs is slow moving and can take many days, requiring the receiving party to agree for the funds to be returned. These issues would make MIP processes inappropriate for attempting to save scam funds (as a scammer will never consent to the funds being returned). A consumer always has the option of contacting the relevant subscriber to seek assistance from a dedicated team.<br><br>**C3Q2**<br>Scenario (a) would allow better consumer outcomes to be achieved as scam transactions would be managed sooner, if they were not required to go through the MIP process. For example, if we detect or are notified of a scam, the scam recovery process commences immediately, where we can issue an indemnity for return of funds. The scam recovery process is quicker than the MIP process, as we send an indemnity for the funds to be returned, and do not have to abide by the MIP process of receipting notifications. A requirement to do this may become more costly for a subscriber.<br><br>We do not agree with the definition in scenario (b). In our view, email hacks/scams should be outside the Code, in instances where a consumer is instructed to make a payment and the details have been purposely changed by a scammer, particularly as the compromise of the account identifiers occurred outside banking systems. Again, we propose that the Code guide subscribers on how to distinguish a push payment scam from a 'MIP'. If a push payment scam is not distinguished from a 'MIP', not only will this be costly as it would extend the scope of the MIP process, but may also result in consumers not being assisted in an effective manner due to the MIP process taking more time. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| **C4** | **On-screen consumer warning** | | |
| | We propose to require ADIs to provide additional important information in the on-screen warning about mistaken internet payments required by clause 25 of the Code. The messaging must:<br><br>(a) contain a 'call to action' for the consumer to check that the BSB and account number are correct; and<br>(b) in plain English, include wording to the effect that:<br>(i) the consumer's money will be sent to somewhere other than to the intended account; and<br>(ii) the consumer may not get their money back, if the BSB or account number they provide is wrong (even if the consumer has given the correct account name). | **C4Q1** Do you support our proposals? If not, why not? | We support the proposal to require ADIs to provide additional important information in the on-screen warning about mistaken internet payments. This is assuming the obligation is in line with that proposed in C4. We do not have any specific comments relating to the wording and agree with what is set out in C4(b).<br><br>There would be a substantial cost to update digital assets across the Group (all brands). This proposal would not carry significant regulatory burdens, as it would also meet AFCA expectations. |
| | | **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? | |
| | | **C4Q3** What costs and regulatory burdens would be involved in implementing the proposed change? | |
| **D1** | **Extending the Code to small business (to be confirmed and redrafted with examples)** | | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | We propose that:<br>(a) The Code will apply to protect small businesses in relation to a subscriber unless the subscriber opts out by notifying ASIC, we publish the subscriber's opted-out status on our website and the subscriber includes notification of its opted-out status in its terms and conditions with small business customers;<br>(b) the Code will apply to small businesses who acquire their facilities in question on or after the date on which the new Code commences (i.e. the extension to small businesses will not operate retrospectively);<br>(c) the term 'user' (referred to in clause 2.1) will be modified to include 'small businesses' and their employees, contractors or agents; and | **D1Q1** Do you support our proposal to provide for an 'opt-out' arrangement for individual subscribers in relation to small business Code coverage? Why or why not?<br><br>**D1Q2** How likely do you think it is that your organisation (if you are a Code subscriber) and other subscribers will opt out?<br>On what grounds might you or other subscribers opt out?<br><br>**D1Q3** Please provide any information you have about the nature and extent of problems for small businesses in relation to electronic payments and about how small businesses would benefit (or not) from having the same protections as individual consumers under the Code?<br><br>**D1Q4** What are the costs and benefits for industry of our proposal? | **D1Q1**<br>We do not support the proposal to provide for an 'opt-out' arrangement for individual subscribers in relation to small business Code coverage. Allowing subscribers to opt-out will create a confusing environment for consumers, and establish inconsistencies and imbalanced burden upon different subscribers, especially within the context of *'reasonable endeavours'*.<br><br>An opt-out arrangement would likely be impractical and costly. Opt-out subscribers would be required to develop processes and functionality to support such an arrangement. For example, the process would need to detect the 'small business' consumer (subject to the definition of this) and treat that particular transaction in a separate manner to a regular consumer. It is also unclear how opt-out subscribers would interact with and manage requests from, or to, opt-in subscribers.<br><br>**D1Q2**<br>We support the extension to small business in principle. It is likely that many of the major financial institutions who are also subscribers would opt-in. However, given the increase in costs to a subscriber which will arise from the Code extending coverage to small businesses, many financial institutions may opt-out, especially with consideration to the broad scope of the proposed definition of small business.<br><br>**D1Q3**<br>Small businesses use sophisticated payment methods and services to initiate electronic payments depending on which option allows consumer benefit (e.g. file based direct entry payments, BPay and Merchant Acquiring). However, often business payment challenges relate to disputed transactions, rather than truly mistaken payments due to businesses often having processes to mitigate these errors. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | (d) after the first 12 months, ASIC will review the number of subscribers who have opted out and will consider options for any enhancements to the experience under the Code for both subscribers and small businesses. | **D1Q5** Do you agree with our proposal D1(b), that the Code should not apply retrospectively to small business facilities already acquired at the time of commencement of the updated Code? If not, why not? What are the costs and complexities versus benefits of our proposal and alternative approaches? | **D1Q4**<br>Assisting consumers to recover funds because of an error is of course beneficial to the consumer. However, given the volume, frequency and complexity of payments made by small business consumers, the costs for industry are largely operational and potentially significant, due to the need for new processes and additional resources.<br><br>**D1Q5**<br>We neither agree nor disagree with the D1(b) proposal as we require further clarity as to the definition of a small business, as well as other requirements under the revised Code. Please refer to our response under D2. |
| | | **D1Q6** What are the key parts of the Code that may present difficulties for subscribers in extending the Code's protections to small businesses? Please provide reasons. | The proposal would likely result in selective application of the Code, which might confuse small business consumers, especially as it appears that the Code may apply to some facilities belonging to the small business consumer but not to other facilities, depending on when it was established.<br><br>The proposal may be costly and complex as some subscribers may opt-out, be required to make a determination as to the establishment date of a facility, be required to make a determination as to whether the consumer fits the definition of a small business and also take action to the extent it be considered *'reasonable endeavours'*.<br><br>While this extended cover under the Code may benefit small businesses in certain situations, the Code may also result in confusion and complaints. The costs for the industry will likely be significant due to the complexities in identifying the commencement date of a facility, in addition to making a determination as to whether the consumer is truly a 'small business'. |
| | | **D1Q7** Does our proposed change to the definition of 'user' (by including employees, contractors or agents of a small) address any concerns about any increased risks to subscribers as a result of extending the Code's protections to small businesses? If not, why not? Do you think this could have any unintended impacts? If so, what are they? | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | **D1Q8** Do you agree that we should review the extension of the Code to small business on an opt-out basis after 12 months? If not, why not? | **D1Q6**<br>We are unable to make a full determination in relation to the key parts of the Code that may present difficulties as we do not have a clear picture of the scope. However, we anticipate the below chapters are likely impacted:<br>• Disclosure requirements<br>• Subscriber liability<br>• Conduct<br><br>**D1Q7**<br>The proposed change to the definition of 'user' provides relief to subscribers as small business consumers often authorise several individuals to operate facilities on their behalf.<br><br>By broadening the definition of *'user'*, more payments may be covered, which will have downstream effects on resources due to an increase in the volume of open 'cases'. For example, workload may also increase as the subscriber would firstly need to determine if the 'user' was authorised to transact on behalf of the consumer.<br><br>**D1Q8**<br>We refer to our response to D1Q1.<br><br>If a subscriber for any reason is given relief by ASIC from including small business when the revised Code become effective, then we agree that ASIC should review this relief periodically. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| **D2** | **Definition of 'small business' (as above)** | | |
| | We propose to:<br>(a) define 'small business' as a business employing fewer than 100 people or, if the business is part of a group of related bodies corporate (as defined in the Corporations Act), fewer than 100 employees across the group, and<br>(b) apply the definition as at the time the business acquires the facility in question (i.e. a point-in-time approach to defining small business). | **D2Q1** Do you agree with the proposed definition? If not, why not? | We do not support the proposed definition of a small business as it extends beyond small businesses with 'consumer like' behaviour, as well as the originally foreshadowed extension of the Code to "sole traders" for which we previously indicated support in principle (and subject to further consultation in defining its application). This definition does not align with that of AFCA or BCoP and would have significant financial and operational implications for subscribers.<br><br>Consumers covered by the proposed definition can be large and sophisticated organisations, with multiple facilities, who may also make a large number of potentially high dollar value transactions. This point in time approach and definition may extend Code coverage beyond its intended consumer base, regardless of how small business is defined. ASIC should also specify the payment types (i.e. limiting coverage 'to pay anyone' payments) and product types (i.e. limiting coverage to basic transaction and savings products) that are covered, to avoid a potentially unquantifiable scope.<br><br>The costs of adhering to the Code with this particular definition of small business would be significant. We do not capture the number of employees a small business consumer has, nor do we have a system identifier for employee numbers. To implement such a change would be a substantial and costly undertaking as a variety of system and process changes would need to be implemented.<br><br>While a consistent definition in line with that of BCoP would be beneficial, we also encourage ASIC to explicitly stipulate which payment methods and product types they are proposing to extend the Code to. This may reduce both the cost and regulatory burden on subscribers, but also provide clarity to both subscribers and consumers. |
| | | **D2Q2** What are the costs and regulatory burden implications versus benefits in setting this particular definition (for example, from a subscriber's system capabilities perspective)? | |
| | | **D2Q3** What alternative definition(s) would you suggest? Why?<br>How do you think the costs and benefits compare to those relevant to our proposed definition? | |
| | | **D2Q4** Given the discrepancy between our proposed definition and AFCA's definition of small business (see paragraph 104), which approach do you think is preferable for the Code? Is there an issue in having slightly different definitions? | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| **E1** | **Clarifying the unauthorised transactions provisions** | | |
| | We propose to adjust the wording of the Code to:<br>(a) clarify that the unauthorised transactions provisions only apply<br>where a third party has made a transaction on a consumer's account without the consumer's consent and do not apply where the consumer has made the transaction themselves as a result of misunderstanding or falling victim to a scam);<br>(b) clarify that the pass code security requirements mean that<br>consumers are unable to disclose their pass codes to anyone<br>(subject to the exceptions in clauses 12.8 and 12.9 of the Code)<br>and, if they do and the subscriber can prove on the balance of<br>probability that the disclosure contributed to an unauthorised | **E1Q1** Do you agree with our proposals? If not, why not?<br><br>**E1Q2** What are the costs or regulatory burden implications flowing from our proposals? Do the benefits outweigh the costs or regulatory burdens?<br><br>**E1Q3** Is it possible for a consumer to input a pass code to a screen scraping service without this amounting to 'disclosure'?<br><br>**E1Q4** Is it possible for consumers to use screen scraping in a way that does not lead to the risk of financial loss? | **E1Q1 & Q2**<br>a. We agree with the wording proposed but it should also be made clear that the unauthorised transactions provisions do not apply to any types of scams.<br>b. We agree with this proposal. In this context "disclose" should have the broadest meaning possible as there are many ways a consumer may disclose their pass code in a manner that may lead to a loss. Where a subscriber does not prohibit the use of a service for accessing a facility, we are concerned that it could be argued there is implicit endorsement. This should not be the case.<br>c. We agree. We also suggest that the Code clearly discloses that the unauthorised transactions provisions do not apply in situations where a scammer gained access through actions completely outside the subscribers' control, such as in situations where the consumer has given or allowed the scammer access to their device and/or disclosed the security password(s) to the scammer.<br>d. We agree with this proposal.<br><br>In addition, there are 'remote access' scams that sit outside of the passcode security requirements, whereby a consumer may be the victim of a remote access scam without disclosing their passcode details. In such cases the subscriber should not be liable. We encourage ASIC to ensure the Code makes this position clear.<br><br>There do not appear to be any particular costs or regulatory burdens associated with the proposal except that if the Code applies to scams and the customer deals |

| | | | |
|---|---|---|---|
| | transaction, the consumer will not be able to get indemnity from the subscriber for that loss;<br>(c) provide some examples of scenarios that amount to express or implicit promotion, endorsement or authorisation of the use of a service referred to in clause 12.9 of the Code;<br>(d) clarify that a breach of the pass code security requirements by itself is not sufficient to find a consumer liable for an unauthorised transaction—the subscriber must, in addition, prove on the balance of probability that the consumer's breach of the pass code security requirements contributed to the loss; and<br>(e) clarify that the provisions concerning liability for an unauthorised transaction are separate to any additional arrangements available under card scheme arrangements (e.g. chargebacks). | **E1Q5** What types of examples involving express or implicit promotion, endorsement or authorisation of the use of a service would be helpful to include in the Code? | with the scammer in a way outside the control or visibility of the subscriber, then the subscriber may bear a considerable financial burden.<br><br>**E1Q3 & Q4**<br>In our view, a customer inputting a passcode to a screen scraping service is a disclosure. Having said this, not all screen scraping services may lead to financial loss. This will always be subject to the security of the website/application of the organisation providing the screen scraping services.<br><br>**E1Q5**<br>By way of example, where a subscriber does not prohibit the service, this may be considered implicit promotion. Additionally, where a subscriber uses a service such as screen scraping, this may also be considered implicit promotion of screen scraping services. However, in our view there are no circumstances in which it should be implied that a subscriber is promoting a particular service. We also note that the challenge for a subscriber is that it is unlikely to know when a consumer uses a screen scraping service therefore, not explicitly prohibiting a service should never be regarded as the subscriber implicitly endorsing that service. This should be acknowledged within the Code. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| **F1** | **Modernising the Code** | | |
| | We propose to:<br>(a) define biometric authentication in the Code; and<br>(b) incorporate biometric authentication into the Code in some specific<br>clauses where required (to recognise that present day transactions<br>can be authenticated by use of biometrics (e.g. fingerprints) where<br>previously only pass codes could be used).<br><br>However, we do not propose to incorporate biometrics into the definition of 'pass code' in a way that would mean that pass codes and biometrics could be used throughout the Code interchangeably | **F1Q1** Do you agree with the proposal to define biometric authentication in the Code? If not, why not?<br><br>**F1Q2** How would you suggest biometric authentication be defined<br>in the Code?<br><br>**F1Q3** Which particular clauses in the Code do you think need to include a reference to biometrics in order for the clauses to continue to have their intended effect?<br><br>**F1Q4** Do you agree that we should not include biometrics in the general definition of 'pass code'? What might be the impacts of taking this approach? In particular, how would using the concepts of biometric authentication and pass codes interchangeably within the pass code security requirements work in practice? What are the | **F1Q1 & Q2**<br>We welcome the proposal to define biometric authentication in the Code, however, 'biometric' information is considered sensitive information under the *Privacy Act 1988* (Cth) (**Privacy Act**), and the inclusion within the Code should not contradict the Privacy Act.<br><br>The definition should be very specific with regard to what types of authentication fall under *'biometric authentication'*, such as facial recognition, voice, gait, and fingerprints.<br><br>The Code should also cater for scenarios where a subscriber permits consumers to only use biometric authentication to authenticate a transaction on a user (that is, where a subscriber replaces the use of pass code with biometric authentication).<br><br>**F1Q3**<br>Clauses 9-14 should contain a reference to *'biometric authentication'*. We would appreciate clarification as to why F1Q3 states 'biometrics' rather than 'biometric authentication' as this may change our position.<br><br>**F1Q4**<br>We agree that *'pass code'* and *'biometric authentication'* should not be defined together. The current definition of pass code includes 'a password or code that the user must keep a secret'. This is not applicable to biometric authentication and in order to avoid confusion, these definitions should be kept separate. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | costs or regulatory burden implications of our proposals? | |
| **F2** | **Defining 'device'** | | |
| | We propose to:<br>(a) revise the Code's use of the term 'device' and instead refer to 'payment instrument'; and<br>(b) include virtual debit and credit cards in the definition of 'payment instrument'. | **F2Q1** Is the term 'payment instrument' more appropriate and easier to understand than 'device? Can you foresee any problems with this terminology? | **F2Q1**<br>We support the modernisation of the Code to more explicitly cater for new products that subscribers are offering (and new features that allow different ways to access and use products).<br><br>However, simply replacing 'device' with a definition of 'payment instrument' that includes virtual cards may not be enough as a virtual card is often just a means of providing information (i.e. card details) to consumers. For example:<br>• there are many references to the term 'device' within the Code that presuppose that it is a thing and these references are not well suited to a definition of payment instrument (e.g. 4.4 & 10.4); and<br>• the description of loss, theft or misuse of a 'device' in the Code and whether this makes sense in the context of a virtual card.<br><br>Consideration would have to be given to the various areas where this term appears in the Code and whether it makes sense in the context of a virtual card.<br><br>**F2Q3 & Q4**<br>More generally and related to the above, the current definition of 'device' only includes devices that a subscriber sends to the consumer, which would not include a phone with a mobile wallet and card details enrolled into it. Where the Code refers to consumers reporting the loss, theft or misuse of a 'device', it is not clear whether the intention would be to extend this to the loss, theft or misuse of a |
| | | **F2Q2** What costs would be involved in industry adjusting to the new terminology? | |
| | | **F2Q3** Are there other new virtual payment instruments that should be covered by the definition of 'payment instrument' or 'device'? | |
| | | **F2Q4** Do you see any unintended consequences from including virtual cards in the definition of 'payment instrument' or 'device'? | |
| | | **F2Q5** What are the costs or regulatory burdens in catering for | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | virtual cards within the definition of 'payment instrument'? | phone. We would welcome further clarification in relation to this potential consequence.<br><br>Subject to the revision of the Code as stipulated in F2, the new terminology may result in significant changes to collateral and 'Terms & Conditions' documents. We are unaware of any new virtual payment instruments that should be covered by the definition, and we do not believe there would be any unintended consequences from including virtual cards in the definition of 'payment instrument' or 'device'.<br><br>**F2Q2 & Q5**<br>There appear to be additional costs or regulatory burdens in catering for virtual cards within the definitions. |
| **F3** | **Payment platforms** | | |
| | We propose to amend the Code to:<br>(a) expressly extend all relevant provisions to situations in which a 'Pay Anyone' payment is made through the NPP; and<br>(b) add a definition of 'Pay Anyone internet banking facility' as a facility where a consumer can make a payment from the consumer's account to the | **F3Q1** Do you agree that the Code's protections should apply to transactions made through the NPP? If not, why not?<br><br>**F3Q2** Are there any particular provisions in the Code that, while workable in the BECS context, would not be workable in the NPP context? What are these and what are your reasons? | **F3Q1 & Q2**<br>We agree that the Code's protections should apply to transactions made through the NPP, and that there are no provisions within the Code that would not be workable in the NPP context.<br><br>**F3Q3**<br>This is possible, as it is a drafting question. One way that this could be achieved, would be to add 'Osko' wherever *'direct credit'* is referred to.<br><br>**F3Q4 & Q5**<br>We support the Code's provisions as relevant, expressly relating only to BECS and the NPP. Other payment platforms will have different characteristics (and may take |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | account of another person by entering, selecting or using a BSB and account number or PayID or other identifier that matches the account of another person. | **F3Q3** Can we accommodate the NPP in the wording of the listing and switching rules in Chapter E of the Code? If so, how? | a different approach to the handling of consumer errors), meaning an agnostic statement will not be feasible.<br><br>We do not foresee any costs or regulatory burden implications relating to F3. |
| | | **F3Q4** Do you support the Code's provisions, as relevant, expressly relating only to BECS and the NPP? Or would your preference be that the Code is payment platform agnostic? What are your reasons? | |
| | | **F3Q5** Do you foresee any costs or regulatory burden implications of our proposals? | |
| **F4** | **Transaction receipts** | | |
| | We propose to amend the Code to cover the provision of electronic transaction receipts as well as paper receipts. | **F4Q1** Do you agree with our proposal? If not, why not? | **F4Q1**<br>We agree with the proposal to amend the Code to cover the provision of electronic transaction receipts as well as paper receipts, insofar as it relates to receipts provided for transactions at the time of the transaction.<br><br>In our view, the proposal will also offer further protection for us and the consumer. However, this would depend on the following:<br>i. the definition of a 'Complete identifier' – perhaps 'Complete Identifier' can be defined within the Code; and |
| | | **F4Q2** Is there any particular information that the Code presently requires to be included on paper receipts that should not be required in electronic receipts? What are your reasons? | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | **F4Q3** What are the costs or regulatory burdens of our proposal? | ii. whether the requirements only apply where the subscriber is the merchant.<br><br>**F4Q2**<br>Clause 5.4(b) may not be relevant to electronic receipts. Furthermore, clause 5.6 may pose an unnecessary security risk, and we question its inclusion even for paper receipts.<br><br>**F4Q3**<br>In relation to the costs or regulatory burdens of the proposal, this would depend upon the requirements the electronic receipts must comply with. If electronic receipts were to comply with the requirements summarised above, this may minimally affect a subscriber who currently issues electronic receipts. If a subscriber, when acting as the merchant, is required to produce electronic receipts, the subscriber may incur substantial costs in establishing such a function. |
| **G1** | **Internal and external dispute resolution** | | |
| | We propose to amend the Code to:<br>(a) replace references to Regulatory Guide 165 Licensing: Internal and external dispute resolution (RG 165) with references to Regulatory Guide 271 Internal dispute resolution (RG 271);<br>(b) combine Chapter F and Appendix A so that complaints | **G1Q1** Do you agree with our proposals? Why or why not? | **G1Q1**<br>We agree with the proposal. Combining Chapter F and Appendix A will drive consistency across both categories. The new Regulatory Guide (RG271) is of a high standard with strict obligations, which should be applied consistently to effectively manage complaints and assist consumers. |
| | | **G1Q2** Are you aware of any particular reasons that may warrant retaining two separate complaints handling frameworks in the Code? | **G1Q2**<br>We are not aware of any particular reasons that may warrant retaining two separate complaints handling frameworks. |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | handling requirements are contained in a single framework instead of two, while retaining important differences in relation to unauthorised transaction report investigations;<br>(c) require all subscribers to have IDR procedures that are set out in<br>RG 271; and<br>(d) require all subscribers to be members of AFCA. | **G1Q3** Do you think we have adequately identified the important differences that require recognition in a merged complaints handling Chapter in the Code? Why or why not? | **G1Q3**<br>We agree that the differences that require recognition in a merged complaints handling chapter have been adequately identified, however note the impact upon subscriber cooperation pursuant to clause A7.1 of the Code. Under RG271, we are required to solve complaints within 30 days, and an extended SLA requirement under the Code may impact upon a subscriber's ability to do so. We are advocating for a shortened SLA, or potentially an exemption from the RG271 timeframe obligation when managing 'cases' affected by A7.1 of the Code. |
| | | **G1Q4** What would be the costs of imposing the same requirements (e.g. AFCA membership, setting up complaints frameworks, disclosure) on all subscribers? | **G1Q4**<br>The costs of the proposal in G1Q4 would vary depending on the size of the subscriber. AFCA currently imposes three types of cost:<br>i. User Base Charges (based on the size of an organisation and the volume of complaints);<br>ii. Membership per entity; and<br>iii. Case management charges (these increase in price as the case process through the AFCA process).<br><br>We do not believe there will be any additional impact as we are already a member of AFCA. |
| **H1** | **Aligning requirements with the Australian Consumer Law** | | |
| | We propose to align the facility expiry period in the Code with the expiry period in the Australian Consumer Law, which is 36 months. | **H1Q1** Do you support this proposal? Why or why not? | We do not object to ASIC's position based on the assumption that the definition of a 'facility' does not include credit cards and debit cards. Our conclusion on this is based on the carve out in clause 18.2 of the current Code referencing 'refunds' which suggests that a 'facility' relates to pre-paid products such as gift cards as referenced in paragraph 179 of CP341. |
| | | **H1Q2** Are you aware of any types of facilities subject to the Code that are not subject to the Australian Consumer Law expiry | |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | date requirements? Should the 36-month expiry date period also apply to those facilities? Why or why not? | Our no objection position is based on the assumption that the definition of a 'facility' as referenced in H1 will not be expanded or changed and that the proposal is merely to align with the ACL requirements and scope, regarding gift card products. |
| | | **H1Q3** What are the costs or regulatory burdens of our proposal? | The expiry period under the Australian Consumer Law only applies to gift cards supplied to consumers in trade or commerce whereas the expiry period set out in the current Code applies more broadly. This distinction may be relevant where subscribers provide facilities to consumers on behalf of certain types of third parties, such as Government agencies. These third parties may have a view on whether the 36-month expiry date period should apply to facilities that are not supplied in trade or commerce. |
| **I1** | **Transition period** | | |
| | We propose to apply an appropriate transition period before the updated Code commences. The specific period will be guided by submissions to this consultation paper. | **I1Q1** If each of ASIC's proposals 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? | **I1Q1**<br>If each of the proposals were to be implemented in the updated Code, we believe an appropriate transition period of at least 18 months should apply. Subject to the changes, we anticipate that the proposals in C1, C4, D1, D2, F2 and F4 would require either significant technological, collateral work, or carry a significant operational impact. |
| | | **I1Q2** Could you provide details as to where each proposal sits on a scale, compared to the other proposals, in terms of the amount of time that is needed for transition? Please provide | **I1Q2**<br>All items below are indicative and subject to ASIC providing further detail and scope with regard to the proposals within this document. The required time needed may vary significantly, depending on the changes to the Code.<br>• Proposal B1: 6 months<br>• Proposal C1: 6 – 18 months |

| ASIC | | | Westpac Group |
|---|---|---|---|
| **ASIC Reference** | **ASIC Proposal** | **Feedback Requested** | **Westpac's Feedback** |
| | | anticipated timeframes, where possible. | • Proposal C2: 6 – 6+ months<br>• Proposal C3: 6 – 6+ months<br>• Proposal C4: 12 – 18 months<br>• Proposal D1 & D2: 18 months<br>• Proposal E1: 6 months<br>• Proposal F1: 6 months<br>• Proposal F2: 6 – 12 months<br>• Proposal F3: 6 months<br>• Proposal F4: 6 – 12 months<br>• Proposal G1: 6 months<br>• Proposal H1: 6 months<br><br>**I1Q3**<br>The proposals that would require significant consideration would be C1, C4, D1, D2, F2 and F4 and refer to the corresponding response. |
| | | **I1Q3** What are the particular costs (in terms of financial and other resources) that ASIC should be aware of in setting a transition period for commencement of the updated Code?<br>Are there considerations that we need to make for particular categories of subscribers? Please be as specific as you can. | |