Jennifer Lyons
Senior Lawyer
Deposit Takers, Credit and Insurers
Australian Securities and Investments Commission
Level 7, 120 Collins Street
MELBOURNE
VICTORIA 3001

2 July 2021

By email only: Jennifer.Lyons@asic.gov.au

Dear Ms Lyons

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the Australian Security and Investment Commission's (ASIC) consultation paper 341 '*Review of the ePayments Code: Further Consultation'*, continues to support ASIC's ongoing review of the ePayments Code (the Code), and thanks you for the ongoing engagement.

We note that this consultation paper is the second of two papers that will form part of ASIC's review of the ePayments Code, in addition to further informal consultation with stakeholders which has taken place in the time since the first consultation paper 310, for which we have participated and previously provided responses. Consequently, whilst we have sought to address all of the issues and proposals raised by ASIC, we have focused on providing more detail around those where the industry consensus indicates there is a need for further discussion and consideration.

A - Mandating the Code

ASIC's position A:

- *"The proposals in this paper reflect the interim nature of our review of the Code in its voluntary form and are designed to ensure the Code is relevant and effective in the short to medium term. The positions set out in this consultation paper, and those ultimately in an updated voluntary Code, may be revisited when the Code is mandated at a future date."*

AusPayNet Members are supportive of the mandatory application of the Code on the proviso that the Code's content would be further reviewed prior to the Code being mandated. On that basis we are supportive of mandating the Code, particularly as and when it applies to new technologies and the wider community of Payment Services Providers at a future date. AusPayNet Member feedback on this issue demonstrated a clear desire for the Code, once reviewed and mandated, to be extended to all payment providers, specifically noting the importance of extending the application of the Code to digital platforms and new entrants.

B - Compliance Monitoring and Data Collection

ASIC Proposal B1: Compliance and industry monitoring

- *We propose to remove the requirement in the Code for subscribers to report annually to ASIC on the incidence of unauthorised transactions. Instead, the Code will include a power that will allow ASIC to conduct targeted ad hoc monitoring of compliance with the Code and other matters relevant to subscribers' activities relating to electronic payments.*

As was outlined in our response to CP310, Clause 44.1 of the Code requires subscribers to provide ASIC with specified information about unauthorised transactions each year. ASIC issued *Information Sheet 195 ePayments Code: Reporting data on unauthorised transactions* to assist subscribers with this obligation. Unauthorised transactional data was reported to ASIC for the years 2015, 2016 and 2017. However, a temporary pause on reporting has been in place since 2018.

AusPayNet Members are generally supportive of the proposal to no longer require subscribers to submit unauthorised transaction data on an annual basis, as it may avoid duplication for subscribers already providing such data to third parties; and given the production of such data, can be resource intensive for the smaller institutions.

The Code currently contains targeted compliance monitoring that allows for 'check ins' on various obligations. AusPayNet supports retaining this approach, provided timeframes and data requests are appropriate and not overly burdensome and that ASIC continues to consult with subscribers prior to engaging an agent to perform compliance monitoring, in line with Clause 44.3.

Going forward, if ASIC were to remove ad hoc monitoring from its remit completely AusPayNet Members are generally in support of the idea that the industry should have a centralized body that collects such data.

In response to the specific questions raised in CP341:

B1Q1 Do you support the removal of the requirement in clause 44.1. If not, why not?

AusPayNet Members are supportive of the removal of the requirement.

B1Q2 What are the costs to subscribers of ASIC continuing an annual collection of data on unauthorised transactions? What would be the costs of setting up and maintaining such an initiative?

Reinstating the annual requirement would be likely to increase costs to subscribers and lead to duplication of reporting requirements.

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?

This would be possible, subject to further industry consultation to establish a mutually suitable reporting body and to avoid duplication. AusPayNet could perform this role, given related and active collection of data in relation to cards, cheques, and digital payments. Subscribers have also indicated that – for the four largest Australian financial institutions (and selected others) – all key transactional frauds are submitted to the Australian Financial Crimes Exchange (AFCX), for the purposes of collating losses and extracting and sharing relevant intelligence. On that basis ASIC could look to obtain such information from either of the above sources. AusPayNet would welcome the opportunity to further discuss with both ASIC and stakeholders as to the part that it could play in this process.

B1Q4 Do you support the additional monitoring or surveying function in proposal B1(b)(ii)? If not, why not?

Yes, provided it did not create additional administrative burden for subscribers or result in duplication with other reporting requirements.

B1Q5 What are the expected costs to subscribers of the additional monitoring or surveying function mentioned in proposal B1(b)(ii)?

AusPayNet Member responses to this question ranged from "nominal" to the cost of 0.3 FTE (i.e., $30k-$50k).

C- Clarifying and enhancing the mistaken internet payments framework.

ASIC Proposal C1: Partial return of funds

- We propose to extend the mistaken internet payments (MIP) framework in the Code to allow consumers to retrieve partial funds if the full amount of the payment is not available in the unintended recipient's account

AusPayNet Members are supportive of the extension of the MIP framework to retrieve partial funds if the full amount of the payment is not available in the unintended recipient's account. Some Members did note however that they would like some further clarity regarding:

- Whether subscribers would retain any discretion as to whether to apply the process for attempting a partial refund.
- Whether there would be a threshold minimum that could be recovered as a "partial retrieval".
- Whether ASIC intends to set a minimum amount that should be left in a customer's account (i.e. to avoid the possibility of overdrawing the account).
- Whether there would be a limit on the number of "partial recovery" attempts from a single account.
- The required frequency and duration of follow-up with the unintended recipient following partial recovery.
- Room for discretion to take into account customer circumstances such as hardship or where the customer was the recipient of Centrelink payments.
- Who would bear ultimate liability for the shortfall.

AusPayNet Members are also supportive of clarifying the concept of "reasonable endeavors" via a non-exhaustive list of examples (as referred to in question C1Q3) and would welcome the opportunity to work with ASIC further on shaping these.

In addition, some subscribers noted that this approach still leaves the outcome open to AFCA's discretion, based on the individual circumstances of each case, so does not automatically determine an outcome. To that extent, the Code should state that the non-exhaustive list is intended as guidance only and is not necessarily indicative of how a later complaint may be determined.

In response to the specific questions raised in the consultation paper:

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?

Generally no, but please refer to comment above in relation to Centrelink payment recipients.

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

Yes, there may be benefits in limiting/minimising the sending consumer's loss and reducing the time taken to retrieve funds (albeit partially).

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?

Yes, the consensus appears to be that the term "reasonable endeavours" is broad and open to interpretation in its current form. Providing a non-exhaustive list of examples will clarify expectations for ADIs, particularly where funds are unavailable. AusPayNet also refers to the comments in the introductory section above.

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

Currently the only example in the Code is in section 32.1 referencing facilitating instalment payments. It would be useful to clarify expectations on the receiving ADI in instances where the unintended recipient:

- Is non-responsive to receiving ADI requests, including how many repeated attempts to make contact, and by what channels, constitutes "reasonable".
- Is not agreeable to repayment by instalment.
- Proposes an impractical repayment plan (e.g. over 20 years).
- Closes the account to which the funds were sent, but still has other accounts with the ADI.

In addition, AusPayNet Members wished to seek further clarity on what steps the receiving or sending ADI can take to mitigate the risk of a complaint being made against it.

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

- Responsiveness and/or ability to contact the unintended recipient by the receiving ADI.
- Status of the account into which the funds were deposited (e.g. closed).
- Availability of funds.
- Establishment of the true nature of mistaken payment.
- Where the recipient is on the bank's sanctions list or a "watch list", in which case the recipient should not be contacted to avoid contravening the no-tipping off provisions of the AML/CTF Act.

C1Q6 Are there any practical impediments to implementation of the proposals to allow the partial recovery of funds?

Generally no, however consideration should be given to:

- Any additional obligations which may be indicated by the non-exhaustive examples of "reasonable endeavours".
- Relevant timeframes for establishing the existence of a MIP where the recipient account holder is overseas or in the case of a deceased estate.

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

AusPayNet Members identified the costs to extend the framework to cover partial return of funds as including:

- Costs of design and implementation of process and system changes.
- Collateral changes and additional collateral.
- Additional labour to send communications to other ADIs and monitor responses in cases where a partial return has been possible.

ASIC Proposal C2: Responsibilities of sending and receiving ADI's

- *The Code would include a non-exhaustive list of examples of what a receiving ADI can do to meet the requirement to make 'reasonable endeavours' to retrieve the consumer's mistaken internet payment (while acknowledging that what amounts to 'reasonable endeavours' depends on the individual case).*
- *There would be a number of additional responsibilities on ADIs to ensure that the process starts promptly and that consumers are made aware of their rights to lodge a complaint with the subscriber and then with the Australian Financial Complaints Authority (AFCA).*

AusPayNet and its Members are supportive of the inclusion of a non-exhaustive list of examples for receiving ADIs (as outlined above).

However, when seeking to clarify the consequences for the sending ADI where the receiving ADI and/or unintended recipient do not co-operate in the process, it was noted that clearly establishing liability is of critical importance to subscribers.

Further consideration should be given to a process initiated by the sending ADI which would require the receiving FI to investigate whether the proper policies and process had been followed in attempting recovery.

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

AusPayNet agrees with the proposed timeframe.

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

AusPayNet Members have provided varied responses; costs vary according to the particular institution.

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

Generally, AusPayNet Members agree these would be of benefit; however, it was noted that current retention methods may need modification to incorporate any new or expanded requirements.

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

AusPayNet Members generally agreed that these could be effectively absorbed within the costs of existing customer communications.

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?

Provided that the concept of what constitutes "reasonable endeavors" is sufficiently clear, the majority of AusPayNet Members agree that the addition of C2(d) would be of benefit.

ASIC Proposal 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.*

AusPayNet is supportive of the proposal to clarify and limit the definition of a MIP so that it only applies to actual "mistakes" and does not extend to scam scenarios.

In making this amendment, further consideration should be given to ensuring that the definition arrived at excludes transactions made to an intended recipient who later turns out to be a fraudulent party (e.g. email compromise scams and authorised push payments.)

AusPayNet is also supportive of ASIC's clarification that it is not proposing to include an account name and number matching requirement for pay anyone transactions using a BSB and account number in its review of the Code. In this regard we would reiterate our earlier comments[1] that industry welcomes support from ASIC to promote existing solutions such as Pay ID which provide better certainty regarding the payee.

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

Yes, please refer to comments above.

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.

(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').

Feedback from AusPayNet Members indicates a clear preference for the definition proposed in subpoint (a). It provides the most regulatory benefit given that it aligns with the earlier discussed concept that the Code is not the right place to deal with scams.

Furthermore, subpoint (a) reflects the industry position that MIPs should not extend to scams. As set out above, consideration should be given to how the definition can make clear that scams are expressly excluded from the MIP regime as the inputting of "incorrect" details could also occur as a result of an authorised push payment scam. The definition should be limited to "actual" or "genuine" input/selection mistakes that are not the result of being provided with false information.

Conversely subpoint (b) seems to cloud the position that the Code is not the appropriate place to deal with scams by making an exception for authorised push payments. This could lead to confusion as to how the Code is to be applied and potentially allow for its application to other types of scams. Whilst a payment made in this

[1] As was discussed at the Industry Roundtable held in February 2021.

scenario could be characterised as a "mistake" because the victim is unknowingly paying an unintended recipient, it is not a genuine mistake of the type described in the Code. because the compromising of the account details occurs outside of banking systems.

AusPayNet Members did not provide feedback as to the relative costs of each approach but may look to do so in their individual submissions where relevant.

ASIC Proposal 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.*

AusPayNet is supportive of the proposal to enhance on-screen warnings and is of the view that this will assist consumers in understanding that they need to take great care when entering payment details.

Whilst prescribing the wording to a degree will help ensure consistency in messaging to customers, AusPayNet is supportive of the approach that wording should be to the "*effect that*" as it will allow ADIs the flexibility to stay "on brand" in their messaging to customers.

AusPayNet would also be supportive of encouraging enhanced consumer and business familiarity and use of the PayID service.

C4Q1 Do you support our proposals? If not, why not?

Yes, see comments above.

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?

As set out above, whilst some prescribed wording or terms may be useful in ensuring consistency between ADIs and assist customer understanding, subscribers should be allowed to remain "on brand" in their communications to customers.

In terms of prescribed wording, it is suggested that ASIC look to more general concepts such as:

- BSB and account details must be correct.
- The payment will not arrive to the intended recipient if the BSB and Account details don't belong to the intended recipient, even if the name used is correct.
- A clear statement that account names were not checked against account details.
- Customers should check that the details they have entered are correct before proceeding with the payment.
- Banks may not be able to recover payments made to the incorrect recipient.

C4Q3 What costs and regulatory burdens would be involved in implementing the proposed change?

In terms of regulatory burden, this proposed change may assist in meeting AFCA expectations and help to facilitate complaints investigations. Some technical changes would be required but these are unlikely to be costly.

D - Extending the Code to small business

ASIC proposal D1: Opt-out arrangement

- *We propose to extend the Code's protections to small businesses, but to provide an opt-out arrangement whereby subscribers may elect not to extend the protections to their small business customers*

AusPayNet Members are generally not supportive of the use of an "opt-out" approach when looking to apply the Code to small business. Our comments and reasoning in this regard are set out below in answer to ASIC's specific questions posed in the consultation.

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?

AusPayNet Members are not supportive of the proposal for an 'opt-out' arrangement in this context as it may lead to inconsistencies between subscribers, which could lead to customer confusion. In this regard we echo the Australian Banking Association's (ABA) comments that the creation of a voluntary regime within a voluntary regime is not an ideal approach.

The relative size of a subscriber and the costs and complexity involved in extending the Code to its small business customers may impact upon its ability to decide to opt-in. This could create division and the potential for competition issues in the market if smaller subscribers are simply unable to opt-in because of cost and resourcing limitations.

D1Q2 How likely do you think it is that your organisation (if you are a Code subscriber) and other subscribers will opt out? On what grounds might you or other subscribers opt out?

AusPayNet is not a subscriber to the Code so has elected not to answer this question.

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?

ASIC's proposed definition is not aligned with banks' customer segmentation and could capture customers with a significant turnover that do not require protection by the Code. Similarly, it could capture complex products which are not compatible with the Code. The inconsistency between ASIC's proposed definition of 'small business' and AFCA's definition may have unintended consequences. Certain small businesses may be contractually entitled to the Code protections but may have no avenue to enforce these protections.

AusPayNet otherwise mirrors the ABA's comments in this regard.

D1Q4 What are the costs and benefits for industry of our proposal?

AusPayNet did not receive any feedback from its Members that would indicate any specific benefit for industry of the proposal in its current form and otherwise indicates support for the comments made by the ABA in this regard.

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?

We need a better understanding of why ASIC is looking to apply the Code in this manner and would benefit from further information and discussion on this point. Feedback received indicates that there are some complexities involved in basing the application of the Code on the time a facility was acquired as opposed to when the actual incident experienced by the customer occurred.

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.

As per D1Q3 above and otherwise mirror the ABA's comments in this regard.

D1Q7 Does our proposed change to the definition of 'user' (by including employees, contractors or agents of a small business) 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?

As per D1Q3 above and otherwise mirror the ABA's comments in this regard.

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?

AusPayNet is generally not in support of the opt-out provisions proposed and otherwise refers to ABA's comments in this regard.

ASIC proposal D2: Definition of 'small business'

- *We propose to extend the Code's protections to small businesses, but to provide an opt-out arrangement whereby subscribers may elect not to extend the protections to their small business customers*

AusPayNet Members are not supportive of the proposal to extend the Code to small business in its current form. The current proposal goes beyond the originally foreshadowed extension of the Code to "sole traders" for which we previously indicated support in principle, subject to further consultation in defining its application.

If the policy rationale is protecting small business because they are 'consumer-like' and can be equally as vulnerable, consideration (outside of the number of employees as proposed) should be given to a cap beyond which it would not be appropriate for a "small business" to be covered by the Code. Whilst we agree the number of employees a business has can be indicative of its size and scope, such parameters in isolation may not necessarily reflect its activities from a payments perspective. In addition to the employee cap, consideration should be given to factors such as the volume or monetary value of transactions or looking to align more closely with existing definitions (in particular AFCA).

A related consideration is whether the definition of a small business for the purposes of the Code would allow the business to be reliably identified as a small business that operated in a consumer like manner and provide sufficient flexibility for re-classification when these businesses evolve in size and operation. Also of concern is the fact that there are differences between subscribers.

Any extension of the Code to small business can have implications for products that are currently not covered by the Code (for example, Commercial Cards, Merchant Acquiring, HICAPS) but with a significant customer base in small businesses. Therefore, specific consideration needs to be given to the intended use cases of the Code's application with this type of customer.

The implications for consumers will also need to be considered and clarified. In many cases, consumers protected by the Code are dealing with small businesses. As such ASIC would need to ensure the provisions for small businesses relate to them consuming these services, not as providers of the services to consumers.

In response to the specific questions raised by ASIC in CP341 AusPayNet responds by way of the matters raised above and otherwise mirrors the positions outlined in the ABA submission.

D2Q1 Do you agree with the proposed definition? If not, why not?

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? 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?

E - Clarifying the unauthorised transactions provisions

ASIC proposal E1: Proposed clarification of the provisions:

We propose to clarify that:

- *the unauthorised transactions provisions of the Code apply only where a third party has conducted a transaction without the consumer's consent;*
- *a breach of the pass code security requirements by itself is not sufficient to find a consumer liable for a transaction (the consumer must have contributed to the loss); and*
- *the protections available under the Code are separate to the chargeback processes available through card schemes*.

AusPayNet is supportive of the proposal to clarify the unauthorised transaction provisions of the Code as proposed.

In particular we are supportive of the proposal to clarify the definition of an unauthorised transaction to situations where a third party has conducted a transaction without a consumer's consent. At a high level we have received mixed feedback (discussed in more detail below) regarding the idea that the Code may still have a role to play as concerns remote access scams, to the extent that such transactions are characterised as being 'unauthorised'. We are of the view that further discussion and guidance around this issue within the Code itself would be of benefit.

As concerns Pass Code Security requirements, we agree that the proposal to clarify that consumers are unable to disclose their passcodes is a positive step. Consideration should also be given to the manner in which voluntary disclosure may occur and what would amount to recklessness on the consumer's behalf. One main theme which has arisen is the issue of establishing liability and the issues encountered by subscribers in

satisfying the balance of probabilities test. Subscribers have previously expressed concerns regarding the application of this test in circumstances where they are predominantly reliant on the information provided by the customer to establish whether a transaction was authorised.

In both cases, whilst it is evident that the provisions of the Code exist to protect consumers, some subscribers have expressed concerns with the existing provisions, stemming from disparities in how the test is applied, and issues in relation to the weight given to the evidence provided by subscribers as opposed to that provided by consumers. Such concerns may be mitigated by continued, non-technical guidance within the Code around processes, liability and subscriber and consumer obligations, that are clear and able to be consistently applied.

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

Yes, AusPayNet Members are generally supportive of the proposals with the exception of some of the issues raised above and below concerning the inclusion of remote access scams and the issue of disclosure within pass code security requirements (PSR).

In the context of PSR, "disclose" should be given a broad meaning as there are many ways a consumer may disclose their pass code in a manner that may lead to a loss. It was noted that AFCA applies similar principles to define Remote Access events as frauds (not scams), which brings them within the ambit of the Code.

Where ASIC does not ultimately define 'disclose' with the broadest possible meaning, there may be an opportunity to review some scam scenarios to determine whether generic wording can be documented, that could permit a partial bank, partial customer liability.

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

AusPayNet Members have indicated that the benefits of the proposal appear to outweigh any associated regulatory burdens or costs.

E1Q3 Is it possible for a consumer to input a pass code to a screen scraping service without this amounting to 'disclosure'?

Broadly, there is an inherent risk when customers share their credentials with third parties. AusPayNet Member feedback indicates however that there may be some circumstances where a customer may input a pass code to a screen scraping service without the action amounting to 'disclosure'. Such a service may also be used in a way that does not lead to a risk of financial loss. However, this is subject to the security of the website/application offering the service, which is not something that consumers are often able to establish until the use of a screen scraping service has resulted in a loss.

With that in mind it would be preferable that consumers continue to be educated on the risks associated with screen scraping services and how this may impact their ability to recover an unauthorised transaction.

E1Q4 Is it possible for consumers to use screen scraping in a way that does not lead to the risk of financial loss?

Please see response to E1Q3 above and in addition we note that:

The Consumer Data Right (CDR) provides an alternative mechanism that enables consumers to share data with accredited parties. For clarity, data sharing under CDR does not constitute screen scraping. The CDR regime enables customers to share their data through secure Application Programming Interfaces (APIs).
Currently, the key steps in this process at a high level are:

i. Customers provide their consent to an accredited data recipient (often a *fintech* or another Bank) to request data relating to them from a data holder on their behalf.
ii. Customers are then redirected to a secure Bank portal where they provide authentication information to that Bank; and
iii. Once they have been successfully authenticated, customers authorise the Bank to share specific data sets through the relevant APIs with the accredited recipients, who hold an 'active' consent from the customer.

The data provided in this way comes directly from the Bank's source systems, rather than screen scraping, and mitigates any risk of financial loss.

Some subscribers have recommended that over time screen scraping should be phased out as has been mandated in the UK and EU markets.

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?

Where subscribers do not expressly prohibit the use of a service, it could be argued there is implicit endorsement. Subscribers can mostly prohibit the use of such services, as it is possible to tell if a customer is using these services by the IP addresses that logins originate from.

F - Modernising the Code

ASIC proposal F1: Biometrics:

- *Define biometric authentication in the Code and incorporate it into specific provisions of the Code where it is relevant;*

AusPayNet is generally supportive of ASIC's proposal to modernise the Code on the basis that the Code should be kept current and up to date as technologies for the authorisation of electronic payments evolve. Alongside this, it is important to strike a balance that allows for technological neutrality. That said, in specifically seeking to define 'Biometrics', AusPayNet Members have indicated a need for further clarity around the problem ASIC is trying to solve for, along with the potential impact of the relevant provisions which may be affected. In particular, the issue of unauthorised authentication by a third party was raised and how the existing liability provisions of the Code might be expanded to cater for such situations. We recommend that ASIC undertakes further discussions with industry on this issue before arriving at any proposed drafting.

If steps are taken to define 'Biometrics' within the Code, consideration should be given to the outcome of the Australian Government's review of the Privacy Act 1988. In addition, ASIC should look to align any definition of biometrics with reference to existing standards. We would welcome the opportunity to discuss this in more detail with ASIC and to enable us to consult more fully with our Members (in particular within the Issuers and Acquirers Community) on this issue.

F1Q1 Do you agree with the proposal to define biometric authentication in the Code? If not, why not?

Generally yes, but noting the issues raised above and provided that it is clear for consumers.

F1Q2 How would you suggest biometric authentication be defined in the Code?

We refer to our comments in the section above regarding alignment with the Privacy Act 1988 and other industry standards.

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?

Anywhere that references passcode or privacy requirements.

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

Given the fast pace at which identification and authentication technologies are evolving ASIC should consider how the Code can remain technology neutral to ensure that it remains relevant in the coming years without needing to be consistently updated and reviewed. Industry would welcome further consultation from ASIC on the intended outcome and how this could be most effectively captured in the Code.

ASIC proposal F2: Defining 'device'

We propose to:

- *(a) revise the Code's use of the term 'device' and instead refer to 'payment instrument'; and*
- *(b) include virtual debit and credit cards in the definition of 'payment instrument'.*

Whilst AusPayNet is supportive of taking steps to modernise the Code to more explicitly cater for new products that subscribers are offering, this proposal should be given further industry consideration, to ensure technological neutrality and relevance in the future. This is of particular relevance in circumstances where the term 'device' has a settled meaning in the payments industry which may not be properly reflected in the term 'payment instrument'.

As with the issue of Biometrics above, we would welcome further information from ASIC as to the problem it is trying to solve for so that we may obtain more detailed feedback from our Members.

F2Q1 Is the term 'payment instrument' more appropriate and easier to understand than 'device? Can you foresee any problems with this terminology?

Simply replacing "device" with a definition of "payment instrument" that includes virtual cards may not be enough. For example:

- As above, it may not be technology neutral, nor future proof;
- There are many references to the term device within the Code that presuppose that it is a thing and are not well suited to a definition that includes information (e.g. 4.4 & 10.4); and
- Query how the Code might go about contextualising the concepts of loss, theft, or misuse of a 'device' in the context of a virtual card.

The new terminology may result in significant changes to 'Terms & Conditions' documents.

F2Q2 What costs would be involved in industry adjusting to the new terminology?

There appear to be no additional costs or regulatory burdens in catering for virtual cards within the definitions.

F2Q3 Are there other new virtual payment instruments that should be covered by the definition of 'payment instrument' or 'device'?

Consistent with our recommendations to ensure technological neutrality, AusPayNet is of the view that more detailed consultation is required to ensure that the Code does not become obsolete as payment methods and financial instruments continue to evolve.

F2Q3 Do you see any unintended consequences from including virtual cards in the definition of 'payment instrument' or 'device'?

With reference to our comment above, it is important to ensure that the Code does not preclude future forms of payment or misrepresent current digital forms of payment. Further consultation is required on this matter.

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. More generally and related to the above, the current definition of 'device' only includes devices that are sent to the customer, which would not include a phone with a mobile wallet with card details enrolled into it. So where the Code talks about customers reporting the loss, theft or misuse of a "device", it is not clear whether the intention is now that this would extend to the loss, theft or misuse of a phone.

F2Q4 What are the costs or regulatory burdens in catering for virtual cards within the definition of 'payment instrument'?

Please see response to F2Q2 above.

ASIC proposal F3: Payment Platforms

We propose to:

- *extend the Code's protections to NPP payments*

AusPayNet is supportive of the proposal to extend the Code to NPP payments. Extending the Code to apply to the NPP would increase consistency.

The NPP Procedures and Regulations were written to reflect the Code and anticipated that changes were to be made to the Code so that it would extend to include the NPP at some stage after the NPP go-live date. To that end, this seems like an appropriate time to include it.

F3Q1 Do you agree that the Code's protections should apply to transactions made through the NPP? If not, why not?

Yes, as per comments above.

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?

None identified at present, but this may need to be given further consideration.

F3Q3 Can we accommodate the NPP in the wording of the listing and switching rules in Chapter E of the Code? If so, how?

Yes, but this will be a question of drafting. One suggestion is to add a reference to NPP Transactions and then list any specific exceptions (e.g., BPAY) wherever "direct credit" is referred to.

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?

We support that the Code's provisions as relevant for pay anyone should only extend to BECS and NPP at this time. Each platform has different characteristics, so an entirely agnostic treatment is not feasible without more detailed consideration. If the Code is mandated, we would recommend that consideration be given to how good principles could be put in place to allow it to work at rail agnostic level.

F3Q5 Do you foresee any costs or regulatory burden implications of our proposals?

No foreseeable costs or regulatory burdens were identified.

ASIC proposal F4: Transaction receipts

We propose to:

- *include electronic receipts in the Code's provisions relating to transaction receipts.*

AusPayNet agrees with the proposal to amend the Code to include electronic transaction receipts while retaining the provisions as concerns paper receipts, noting it will require some technical change.

F4Q1 Do you agree with our proposal? If not, why not?

Yes, as outlined above and in addition note that the proposal will also offer further protection for subscribers and customers.

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?

Feedback received identified the following as potentially not being relevant:

- Type and general location of equipment used or a symbol to identify equipment (if practicable).
- A reference number linking to a merchant issued invoice with the same reference number.
- Balance remaining (even as concerns paper receipts).

F4Q3 What are the costs or regulatory burdens of our proposal?

Privacy considerations are critical to protect customers from having their details revealed to malicious perpetrators.

In relation to the costs or regulatory burdens of the proposal, this would depend on what restrictions the electronic receipts must comply with. If electronic receipts were to comply with the above, this would likely be of minimum impact.

G - Complaints handling

ASIC proposal G1: Internal and external dispute resolution:

- *We propose to amend the Code to require all subscribers to have IDR procedures that are set out in Regulatory Guide 271 Internal dispute resolution (RG 271) and to be members of AFCA.*
- *We propose to combine Chapter F and Appendix A to adopt a single complaints handling framework*

In general, AusPayNet is supportive of the proposal for internal and external dispute resolution, but in circumstances where it is not directly involved in these processes will allow our Members to answer on an individual and more detailed basis. However, we wish to summarise some of the feedback we received to the questions posed in the consultation paper as follows:

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

AusPayNet Members were generally supportive of the proposals in G1(a). As concerns the G1(b) proposal we agree that one single framework will increase consistency across both categories. The new Regulatory Guide (rg271) is of a high standard and contains strict obligations which need to be consistently applied in order to effectively manage complaints and assist customers.

G1Q2 Are you aware of any particular reasons that may warrant retaining two separate complaints handling frameworks in the Code?

AusPayNet Members indicated that they were not aware of any particular reasons that may warrant retaining two separate complaints handling frameworks. Such position being based on the assumption that RG271 does not apply to Appendix A subscribers.

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?

AusPayNet Members generally agreed that the differences that require recognition in a merged complaints handling chapter have been adequately identified, however not the impact upon subscriber cooperation pursuant to clause A7.1 of the Code. Under RG271, subscribers 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 would suggest 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?

AusPayNet Member feedback received indicated that the costs of the proposal in G1Q4 would vary depending on the size of the subscriber. AFCA currently have three levels of cost:

i. User Base Charges (based on the size of an organisation and the volume of complaints).
ii. Membership per entity.
iii. Case management charges (these increase in price as the case process through the AFCA process).

H - Facility expiry dates

ASIC proposal H1: Aligning requirements with the Australian Consumer Law:

We propose to update the minimum 12-month expiry period for certain facilities in the Code to adopt a minimum 36-month period, in line with the Australian Consumer Law.

In general, AusPayNet is supportive of the proposal to align with Australian Consumer Law requirements, but in circumstances where it is not directly involved in these processes will allow our Members to answer on an individual basis.

I - Transition and commencement

ASIC proposal 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

AusPayNet is supportive of the concept that the industry will require a suitable transition period in order to properly incorporate the proposed amendments into its regular compliance practices. Feedback has indicated that a period of 12-18 months would be required, noting that certain amendments may require more time than others to implement (e.g. extension to small business in particular).

Next Steps

AusPayNet understands that the next phase of the review will involve ASIC forming its final positions on updates to the Code. This next phase is expected to include a revised Code for consideration. This revised version of the Code will reflect final positions for stakeholder feedback purely on the format and technical wording and not the policy positions in the Code.

With that in mind and in light of certain issues which we have identified as requiring further industry consideration and discussion, we would welcome the opportunity to engage further with ASIC at any time on the issues raised in this letter, or on broader issues related to the ePayments Code Review. Please contact , AusPayNet Legal Counsel, ( ) if you have any further questions.

Yours sincerely

Chief Executive Officer
Australian Payments Network