

Sent by email to: [ePaymentsCode@asic.gov.au](mailto:ePaymentsCode@asic.gov.au)

11 April 2019

## RE: Review of the ePayments Code: Scope of the Review

The Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the ASIC consultation paper, *Review of the ePayments Code: Scope of the Review*. We note that this is the first of two papers that will form part of ASIC's review of the ePayments Code (the Code), with this paper seeking feedback on the topics to be included in the scope of the review, ahead of a more substantive consultation paper setting out proposed modifications to the Code. Consequently, we have provided feedback at a high level to enable ASIC to set the parameters of the review.

### AusPayNet Membership & Role

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. AusPayNet manages and develops regulations, procedures, policies and standards governing payments clearing and settlement within Australia. Membership of AusPayNet is open to participants in, and operators of, Australian payment systems which are recognised as meeting a set of criteria specific for a membership category.<sup>1</sup>

AusPayNet currently has over 125 members, including:

- a) Financial Institutions (FIs), including the major banks and other Authorised Deposit-taking Institutions (ADIs) including credit unions and building societies;
- b) the Reserve Bank of Australia (RBA); and
- c) Operators or administrators of Australian payment systems including BPAY, Austraclear, Visa, Mastercard, American Express, eftpos Payments Australia Ltd, PayPal and NPP Australia Ltd (NPPA).

AusPayNet's responsibilities include:

- controlling and managing risk in the Australian payments system;

---

<sup>1</sup> Categories of membership are: (i) appointing members; (ii) electing members; (iii) operator members; and (iv) affiliate members.

- co-ordinating the operation of effective payment systems through facilitating industry collaboration, self-regulation and system-wide standards; and
- developing industry policies and rules for the regulation of payment systems (also known as clearing systems) relating to cheques; direct entry (i.e. direct debit/credit); cards and accepting devices (i.e. cards used for in-store purchases at Point of Sale (POS) terminals, ATMs, or phone/internet purchases); high value payments (e.g. between FIs); and the distribution of cash in Australia.

### ASIC Proposal B1: Future Proofing the Code

We propose to assess whether the Code, as currently worded, has successfully adapted to today's payments environment and is sufficiently adaptable to respond to emerging and future developments in financial technological innovation and changing customer behaviour

AusPayNet supports the proposal to assess whether the Code has adapted to, or is sufficiently able to adapt to, reflect and respond to emerging technologies. AusPayNet is happy to offer assistance to ASIC in this assessment, including on those issues identified below:

- **The New Payments Platform (NPP).** AusPayNet established NPPA in late 2014 to oversee the build and operation of the platform. The NPP is a significant piece of national infrastructure and the result of a collaborative industry initiative, designed to meet the needs of the digital economy. It is important to let the NPP develop and mature and we suggest that the Code should be adapted to incorporate the NPP.
- **Mobile and Other Non-Device Payments.** Where the Code currently uses concepts such as device and identifier, it should be updated to ensure that the same provisions that rely on those concepts also cover electronic payments made without such a device/identifier (e.g. card-on-file, in-app and tokenisation).
- **Biometric Authentication.** Protections under the Code that apply to the use of a pass code (e.g. a PIN) should also apply to biometrics: they are simply another method for verifying a customer. In addition, we submit that this should also apply in the case of e-commerce digital payments (authenticated through multi-factor authentication).
- **Transaction Receipts.** The Code provisions applying to receipts should be reviewed in the following aspects: to ensure that the Code applies to all forms of receipts sent electronically, not just paper receipts; to ensure that sensitive information is omitted from all forms of receipts; to ensure that the types of information required on the receipt (such as cl. 5.4(b) equipment type for online and mobile transactions) are still relevant and useful; to ensure that provisions affecting receipts (including clauses 5, 21, and 22.1(c)) are located together or reference each other; and to provide consistency for consumers regarding their rights to a receipt under the Code having regard to other laws applying to proofs of transaction and electronic communication<sup>2</sup>.

<sup>2</sup> For example, s100 of the Australian Consumer Law, and the Electronic Transactions Act 1999.

## ASIC Proposal B2: Complaints Handling

We propose to assess the clarity and appropriateness of the current policy positions in the Code's complaints handling provisions

AusPayNet supports this inclusion in the scope of the review, on the proviso that it is with the aim of reducing complexity for consumers and subscribers, avoiding duplication, and having consistent application to all subscribers.

## ASIC Proposal B3: Unauthorised Transactions

We propose to assess whether the current settings in the Code for unauthorised transactions are appropriate and sufficiently clear

Clarifying liability and timeframes in which to bring a claim for unauthorised transactions should be a priority for this review.

Recommendation 17.6 of the Productivity Commission (PC) Inquiry, *Competition in the Australian Financial System*, stated (in part):

- *ASIC should more clearly define the liability provisions for unauthorised transactions when third parties are involved, including participation in financial dispute resolution schemes.*<sup>3</sup>

The Australian Government has committed to introducing open banking, as the first tranche of an economy-wide consumer data right (CDR). Sharing of consumer data via APIs is due to commence in February 2020.<sup>4</sup> One of the features of the CDR is a higher level of consumer protection, via the Privacy Safeguards.<sup>5</sup> This is in contrast to the practice of screen-scraping, which was described by the independent Treasury Report, *Review into Open Banking in Australia*, as “risky, unstable and costly.”<sup>6</sup> The PC also noted that screen-scraping may leave the customer liable for unauthorised transactions initiated by the third party, and this “has led to uncertainty among consumers about whether they are protected.”<sup>7</sup>

Given that the Australian Government and the banking sector are working to deliver an open banking regime, account aggregators should switch to utilising APIs, rather than screen-scraping. Sharing data in a framework which has clear operating standards, including liability allocation, would provide better security for consumers and remove the need to share login details. Since alternatives to screen-scraping will be available, the Code should maintain the principle that subscribers and consumers should be liable for their own conduct, and that a consumer who breaches pass code security carries liability for any data breach.

---

<sup>3</sup> Productivity Commission, *Competition in the Australian Financial System*, Recommendation 17.6, p504

<sup>4</sup> Treasurer the Hon. Josh Frydenberg MP, Press Release: *Consumer Data Right Rules, Standards and Timelines*, 21 December 2018

<sup>5</sup> Treasury, Fact Sheet, *Consumer Data Right Privacy Protections*

<sup>6</sup> Treasury, *Review into Open Banking*, December 2017, p72

<sup>7</sup> Productivity Commission, *Competition in the Australian Financial System*, Draft Report, 7 February 2018, p290

It is important to note that other industry work supplements the Code in improving consumer safety, through education, both on how customers can protect themselves and the liabilities that apply when they do not take advantage of such protections. This is the logic behind initiatives such as AusPayNet's (then-APCA) "Protect Your PIN" campaign, which extend to password protection and biometric use-cases. AusPayNet's *Card-Not-Present Fraud Mitigation Framework* is an example of FIs and wider industry working together to solve fraud and build effective minimum standards – negating the need for the Code to do so.

AusPayNet suggests that the six-year limitation period for customer claims for unauthorised transactions should be reduced, as experience has shown that it is too long a period to allow effective investigation and recovery of customer funds. A 12-month period for a customer to bring a claim after becoming aware of the circumstances of the claim – which would need to be defined – could achieve more reliable and successful outcomes.

The Code can also play an important part in helping customers that are the victims of identity theft or monetary scams. AusPayNet is developing a standard to articulate minimum response measures that payment providers should implement in order to effectively manage identity theft and scam related risks with industry and customers. Complementary provisions within the Code would help establish desired behaviours within the industry, providing consistent levels of support to customers. Alignment between AusPayNet's standard, the Code and relevant provisions in the *Privacy (Credit Reporting) Code*<sup>8</sup> outlining how credit reporting laws deals with fraud will be important to ensure payments providers are guided by consistent requirements and that customers are provided a consistent experience across payment providers. AusPayNet would welcome the opportunity to share the development of this standard with ASIC at the appropriate time.

It is also worth noting that the UK's Payment System Regulator (PSR) has published an *Authorised Push Payment Scams Voluntary Code*, which provides a good example of another jurisdiction addressing these issues.

#### ASIC Proposal B4: Data Reporting

We propose to review the data reporting requirements in the Code and assess the most valuable and efficient approach.

AusPayNet supports that reviewing the Code's data reporting requirements, including unauthorised transactions and card not present fraud, would be useful.

AusPayNet has been publishing industry-wide card and cheque fraud statistics since 2006 as part of the industry's commitment to counter payments fraud.

We collect fraud statistics twice-yearly from Australia's financial institutions and from the major card schemes operating in Australia. The data captures fraud on all Australian-issued payment cards used both domestically and overseas and provides a breakdown by scheme, credit, debit and charge cards, and by proprietary debit cards. The data is categorised under fraud types including card-not-present

---

<sup>8</sup> Maintained by the Office of the Australian Information Commissioner

(occurring mainly online), counterfeit/skimming, and lost and stolen. FIs report card fraud data as gross actual losses.

AusPayNet publishes the aggregated data to help increase awareness about fraud trends, prevention and security, and to assist financial institutions in monitoring fraud trends and developing targeted mitigation strategies.

AusPayNet would welcome working with ASIC on this area of data reporting to assess the most valuable and effective approach and avoid duplication of reporting obligations.

### ASIC Proposal B5: Mistaken Internet Payments

We propose to consider whether the provisions in the Code for mistaken payments are simple and accessible enough, and whether ADI subscribers should have any role in mitigating or preventing such payments.

AusPayNet agrees that customers who have genuinely made a mistake in sending an internet payment should have a simple and accessible process to assist in seeking recovery of the payment. The current regime, as outlined in the Code, provides the sender of the mistaken payment an avenue to report the mistake and seek to have the funds returned. AusPayNet administers the framework for the Bulk Electronic Clearing System (BECS) for electronic debit and credit payment instructions. The BECS framework co-ordinates and facilitates the exchange and settlement of bulk electronic transactions between participants. Direct entry is used for such payments as internet banking transactions and direct debit and direct credit instructions. It is generally used for smaller day-to-day payments but is available for payments up to \$100 million. Payments collected from customers' bank accounts are "direct debits" and payments sent to customers' bank accounts are "direct credits".

The BECS Procedures contains a regime for ADIs to follow when a mistaken payment is made, which is aligned to the Code.

The consultation paper states that stakeholders have noted that "the intended recipient who did not receive the payment cannot seek return of the payment through the sending or receiving ADI." Introducing a regime where the intended recipient can initiate the process requires careful consideration. This includes ensuring that privacy requirements are met along with achieving successful outcomes for both senders and receivers of payments. AusPayNet agrees that the process could be simplified and supports a review to ensure there is a shared understanding about the application of the process across industry and regulatory bodies. AusPayNet's forthcoming consultation on the future of Australia's payment rails, including BECS, is one potential input to such a review.

As the consultation paper notes, the growth in registration and use of PayIDs is likely to reduce mistaken payments over time.

AusPayNet is of the view that on-screen warnings provided by sending FIs continue to have a role to play in assisting customers. We agree that the Code should require that such warnings expressly warn customers that correctly entering the account name will not fix an incorrect BSB or account number.

The consultation paper also refers to the three-part process for recovery of the mistaken payment, of which the first category are payments reported within 12 business days. AusPayNet notes that clauses 28 and 29 of the Code (and the equivalent provisions in the BECS Procedures) refer to the period of 10 business days.

Finally, the Code currently excludes certain payments from the definition of a mistaken internet payment, where a payment scheme has its own rules for mistaken payments handling. This exclusion should be reviewed to ensure that it comprehensively applies to all payment schemes which have their own rules for mistaken payments handling.

### ASIC Proposal B6: Small Business Access to Code Provisions

We propose to explore whether it may be appropriate to extend the Code, or at least some of its protections, to small business.

As the paper acknowledges, this matter requires considerable further analysis including an appropriate definition and a threshold test of small business. AusPayNet will provide further detail should ASIC decide to include small business protections in the next stage of the review.

### ASIC Proposal B7: Other Aspects of the Code

We propose to consider any other aspects of the Code that may need updating as part of our review.

The paper notes three other issues that may be relevant: Stored Value Facilities (SVFs); Restricted ADIs (RADIs); and gift cards. AusPayNet provides the following comments:

- **SVFs.** The Code will need to reflect the final version of the regulatory framework currently under development by the Council of Financial Regulators and timetabled for mid-2019 (with APRA then reviewing its regulatory approach to SVFs that fall within its remit in 2020);
- **RADIs.** We agree that these should be out of scope, as RADI licence-holders are not permitted to offer services to the general public. According to APRA's *ADI Licensing: Restricted ADI Framework*, an entity with a RADI licence is restricted in its products and services offerings. RADI customers offered a new product during the restricted phase are expected to consist of staff of the RADI, family and friends of staff, and a small number of early adopters who have expressed an interest in being involved in the start-up phase of the RADI. Other members of the general public should not be able to apply for a new release product from a RADI. As such the Code would not be applicable; and
- **Gift Cards.** We support bringing the expiry date for gift cards in line with the three-year period outlined in the *Competition and Consumer Amendment (Gift Cards) Bill*.
- **Frequency of Statements.** The Code should be clarified where there is misalignment between it and other laws or regulations; for example, clause 7.1 of the Code, and section 33 of the National Credit Code.

In addition to the above, AusPayNet suggests that ASIC should also consider the following aspects in its review:

- Consistency between the requirements and terminology relating to regular payments lists in the Code, the BECS Procedures and the ABA Banking Code of Practice; and

The overall readability of the Code, to ensure that it is simplified and more easily understood, has a logical sequence and any outdated references are removed or corrected. Conclusion

In summary AusPayNet supports:

- Updating the Code to bring it in line with developments in technology, new payment operating models and changes in the ways customers pay;
- Clarifying liability and timeframes in which to bring a claim for unauthorised transactions;
- Reviewing the mistaken internet payments regime to ensure that there is a shared understanding between subscribers to the Code, customers and ASIC about its application and process;
- Rationalising the complaints handling provisions; and
- Reviewing the Code's data reporting requirements.

Finally, consistent with the PC's Recommendations,<sup>9</sup> AusPayNet reiterates its support for the Code to be mandatory for all senders and receivers of payments and to be reviewed on a more frequent basis. We note however that the matter of mandating the Code is not within the scope of the current consultation. As such we will review our support for the Code to be mandatory in the context of ASIC's future, more substantive consultation paper setting out proposed modifications to the Code.

AusPayNet would welcome further discussions with ASIC on any of the matters raised in this submission.

Yours sincerely



Andy White

**Chief Executive Officer**

---

<sup>9</sup> Productivity Commission, Competition in the Australian Financial System, Recommendation 17.6, p504