eftsure Pty Ltd
ABN 21 168 403 736
ACN 168 403 736

Level 6, 122 Walker St,
North Sydney 2060
1300 985 976

eftsure.com.au

2 July 2021

Australian Securities and Investments Commission
By email: ePaymentsCode@asic.gov.au

Dear Sir/Madam

Re: CONSULTATION PAPER 341: Review of the ePayments Code: Further consultation

eftsure welcomes the opportunity afforded by the Australian Securities and Investments Commission (Commission) to provide feedback into proposed modifications to the ePayments Code (Code).

ABOUT EFTSURE

eftsure is a unique Australian fraudtech platform that ensures organisations can process Electronic Funds Transfer (EFT) payments securely, by mitigating the risk of fraud and error. Gaps in Authorised Deposit-Taking Institution (ADI) verification systems result in an Account Name not being matched against a BSB or Account Number when EFT payments are being processed.

This verification gap results in a range of heightened risks for Australian organisations:

External Risks:

Criminal syndicates, often based overseas, use a variety of tactics, such as Authorised Push Payment (APP) or Business Email Compromise (BEC) attacks, to engage in invoice fraud. This involves deceiving Accounts Payable (AP) staff into amending supplier payment details, resulting in funds being erroneously and irretrievably paid into bank accounts controlled by the criminals.

Such fraud ranks as the most common type of cybercrime according to the Australian Cyber Security Centre (ACSC). It represents 39.86% of all reported cybercrimes.[1] In FY 19-20, reports of BEC scams to the ACSC cost Australian organisations in excess of $142 million.[2]

Internal Risks:

Gaps in ADI verification systems can also result in malicious internal actors manipulating supplier payment data in Enterprise Resource Planning (ERP) systems or the text-based Australian Banking Association (ABA) files that are used to process EFT payments in online banking portals. These verification gaps can also increase an organisation's risk of incorrect payments due to human error. This typically occurs when AP staff incorrectly enter payment data manually.

[1] https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[2] https://www.cyber.gov.au/acsc/view-all-content/news/business-email-compromise

Launched in 2016, the eftsure platform helps mitigate these risks by enabling AP functions to cross-check their supplier banking records against an aggregated database comprising nearly 2 million Australian organisations. By verifying that the banking details being used to process EFT payments align with the details used by other organisations when paying the same supplier, organisations gain assurance that their supplier records are accurate. This reduces their exposure to financial losses resulting from fraud or error.

CODE REVIEW

eftsure understands the purpose of this review is to ensure the Code remains relevant and effective. This is an important undertaking on the part of the Commission given the rapid rate of change in payments systems and technologies. Australians need a strong sense of confidence in the security and reliability of electronic payments systems, without which, the full potential of a digital economy cannot be realised.

Whilst the scope of the Code pertains primarily to business-to-consumer (B2C) payments, eftsure believes a number of key matters raised in the review consultation paper also have relevance for business-to-business (B2B) payments.

CLARIFYING AND ENHANCING THE MISTAKEN INTERNET PAYMENTS (MIP) FRAMEWORK
C3: Definition of 'mistaken internet payment'

It is proposed that the Code be amended to clarify the definition of MIP to ensure it only covers actual mistakes, or errors, when inputting account identifiers to make payments. The proposal is to ensure the definition of MIP does not extend to payments made as a result of fraud or scams.

eftsure accepts the view of the Commission that mistsakes arising through human error should be treated differently to instances of fraud or scams.

However, given the rapidly increasing sophistication and incidence of APP and BEC attacks, eftsure views the suggested delay in addressing the challenge of fraud until such time as the Code is made mandatory, to be a missed opportunity.

Whilst it is true that occurrences of error and fraud may demand different responses, depending on the circumstances of each incident, there is nonetheless strong alignment in terms of the measures that can be implemented to prevent both risks. This review of the Code represents an ideal opportunity to encourage subscribers to adopt measures that will help reduce both error and fraud.

As recognised in the Consultation Paper, ADIs generally do not match an Account Name with the BSB and Account Number when payments are being processed. Nor are they matched to the beneficial owner of the bank account. There are any number of reasons why such matching poses a significant challenge. For example, Account Names may be truncated or abbreviated; utilisation of trusts; a corporate entity may have multiple trading names, each with their own bank accounts; over time, corporate changes, such as mergers and acquisitions, may result in a variety of different entities or subsidiaries with different names.

Comprehensive matching would require significant data sharing across multiple ADIs. This poses a range of complexities, as noted by many in the United Kingdom following the introduction of the 'Confirmation of Payee' initiative.[3]

eftsure recognises that any proposal requiring bank-to-bank data sharing introduces a range of technical and regulatory/privacy challenges and is therefore beyond the scope of this voluntary Code.

Nonethless, the Commission could use the Code to encourage subscribing ADIs and industry to work together in exploring alternate measures to prevent both error and fraud, even if those measures fall short of comprehensive bank-to-bank data sharing. The threat to industry from APP and BEC fraud is becoming so acute, that any preventative measures are urgently required. This is particularly the case for small and medium sized enterprises, for whom the costs of such fraud can be crippling.

Rather than delaying addressing the issue of payments fraud until such time as the Code is made mandatory, the Code should encourage subscribing ADIs to cooperate with other organisations in finding ways to mitigate risks. Payments fraud is not a problem ADIs can solve independently. The tactics used by criminal syndicates, such as Social Engineering, demonstrate that fraud is a whole-of-society challenge, requiring a whole-of-society solution.

For example, ADIs could work with industry to raise widespread awareness of the importance of regularly verifying payment data before processing payments. This would help address both error and fraud.

Furthermore, ADIs should be encouraged to explore potential technical solutions that address the risks of both error and fraud. eftsure's fraudtech platform, whereby data is aggregated from individual organisations, rather than from ADIs, represents a novel and effective approach to addressing this complex challenge.

By encouraging ADIs to work collaboratively with industry players that help minimise and mitigate fraud, such as anti-virus, spam filter and payment protection companies, the Code would be making a significant contribution to uplifting community-wide resiliency against scams. All parties would be the beneficiaries of such an approach, including consumers, businesses, industry and the ADIs themselves, who would avoid reputational damage and enhance client satisfaction.

C4: On-screen consumer warning

It is proposed that the wording used in on-screen warning messages be strengthened. These warning messages are displayed in online banking portals immediately prior to a payment

[3] https://www.openbankingexcellence.org/blog/confirmation-of-payee-what-is-it-why-its-important-and-whats-next/

being processed. The purpose of these warnings is to advise payers that an incorrect BSB or Account Number may result in funds being irretrievably sent to an unintended recipient.

eftsure endorses strengthening warnings about potential loss of funds if incorrect payment data is entered.

Whilst on-screen warnings are important, there is a tendency by many not to pay close attention to them. The fact that erroneous payments, whether due to error or fraud, are increasing, demonstrates the limitations of such warnings.

eftsure believes such warnings should aim to educate the general public about the importance of verifying payment data. If payers were required to actively consent to removing the warning message from the screen of their device, for example by ticking a box, as well as being provided with links to further resources on stopping fraud, either directly or using industry tools, this would attract more attention to the message and make it more valuable in the fight against scams.

---

eftsure thanks the Commission for this opportunity to contribute to this important review of the ePayments Code. Should the Commission wish to further explore any matters raised in this submission, eftsure would be pleased to fully cooperate.

Yours sincerely

Mark Chazan
Chief Technology Officer
eftsure Pty Ltd
eftsure.com.au
1300 985 976