



6 February 2020

Australian Securities and Investment Commission
C/o Review of the ePayments Code team

By email: ePaymentsCode@asic.gov.au

Dear Sir/Madam

Re: Review of the ePayments Code

We understand the Australian Securities and Investments Commission (ASIC) is reviewing the ePayments Code¹ (Code).

The Australian Competition and Consumer Commission (ACCC) as you know runs Scamwatch (www.scamwatch.gov.au), through which consumers can report scams. We regularly monitor scam reports to understand and raise public awareness about scam trends.

The ACCC often identifies laws and regulations that could be improved to ensure Australians are better protected against scams. We are pleased to provide the following information to assist the review of the Code.

Scams

One of the questions you ask is “What role, if any, could the Code play in preventing or reducing the risk of customers who have lost money to scams?”

As you know, scams are a complex and evolving problem causing substantial financial and emotional damage to every demographic in Australia. Financial losses to scams are growing and impact the whole of the Australian economy, as money stolen by scammers could be otherwise spent in legitimate transactions. Disrupting scams and target hardening is a shared problem for government, the community and the private sector. Regulatory frameworks in the financial sector can provide important protections for consumers, and private organisations should be required to do more to ensure their services, platforms, technology and systems are not able to be exploited by scammers.

The ACCC reports annually on the impact of scams in Australia.² In 2018, Scamwatch received over 177 500 scam reports with \$107 million in financial loss. Combined losses including reports to the Australian Cybercrime Online Reporting Network (ACORN) conservatively exceeded \$489.7 million. Financial service providers should have obligations

¹ <https://asic.gov.au/regulatory-resources/find-a-document/consultation-papers/cp-310-review-of-the-epayments-code-scope-of-the-review/>

² <https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity>

to provide strong detection and preventative measures to assist their customers to protect themselves from scams.

Better protection for scam victims required – UK initiatives

The ACCC's experience in administering Scamwatch highlights the need for better protections for scam victims in Australia. The ACCC recommends that two current initiatives in the UK be considered in Australia. The first is the *Contingent Reimbursement Model Code for Authorised Push Payment Scams* which provides greater protections for scam victims when they 'authorise' a transfer in circumstances where they have been tricked and provides them reimbursement (subject to particular criteria) from a pool of money funded by the banking sector. The second is the *Confirmation of Payee* service that will be compulsory in the UK from March 2020. This is a broader initiative that will assist consumers and businesses to check they have the correct name for the person or business they are paying, give better protection against certain types of fraud, and help to stop accidental mistakes too.

We encourage ASIC to consider how similar initiatives to those in the UK could be implemented in Australia to better protect scam victims, and prevent accidental transfer of money (whether to a scammer or otherwise). The review of the Code may be a mechanism through which similar initiatives could be explored

Contingent Reimbursement Model (CRM) Code for Authorised Push Payment Scams

In May 2019, the UK introduced a new voluntary industry code called the *Contingent Reimbursement Model Code for Authorised Push Payment Scams* (the CRM Code). The introduction of the CRM Code was in response to the £354.3m lost to Authorised Push Payment fraud in the UK in 2018 and the acknowledgment of the huge impact of fraud on individuals and businesses.

'Authorised push payment' (APP) scams is a term used in the UK to describe a range of scams where customers are *tricked* into authorising a payment to an account that they believe belongs to a legitimate payee – but is in fact controlled by a criminal. The scammer or fraudster will often contact the victim via phone, email or social media and pretend to be someone else – such as their bank, a contractor, a utility, an estate agent, the government or even the police.

Generally in Australia these types of scam transactions would not fall within the protections afforded by the 'unauthorised transactions' rules of the Code. In fact, Australians are often unable to obtain redress because they are considered to have 'authorised' the transaction even though they were misled. The UK model adopts more of a 'no blame' approach towards scams. It places the onus on banks to actively identify and warn customers about scams and provides a fair system for redress in appropriate cases. The CRM Code says that if the combination of a person's individual circumstances and the scam itself mean that it wasn't reasonable to expect that person to have protected themselves, then they should always be given their money back.

Currently, the CRM Code is voluntary. The advent of real-time payment schemes in the UK has made push payments more attractive to criminals because they can quickly take the money and run and the money cannot be retrieved. While the deceptions can take any form, examples include dating scams, online shopping scams or a scammer posing as someone who has been employed by the victim and sends fake invoices to get the victim to send money to them and other forms of business email compromise or false billing scams. An authorised push payment will include a payment where, as part of giving consent for a specific payment, a customer shares access to their personal security credentials or allows

access to their banking systems such as online platforms or banking apps for that payment to be made.

The CRM Code includes a fundamental principle that when a customer has been the victim of an APP scam payment service providers should reimburse the customer. However, the CRM Code includes a number of exceptions, for example where the customer ignored effective warnings. The CRM Code also provides for reimbursement (regardless of the exceptions) if a victim is assessed as being vulnerable to APP scams.

The CRM Code also sets out a mechanism whereby the sending and receiving payment service providers allocate between themselves the cost of reimbursing the victim of the APP scam and contribute to a “no blame” fund.

We understand that the current UK funding arrangement is due to expire in March 2020 and that the government and industry are working on a longer term arrangement for the future. Data on reimbursements under the code is due to be published this year.

Payee/Account name checks – bolstering protections for mistaken payments and fraud

Similar to current practice in Australia, banks in the UK are not currently required to check the account name when sending an electronic payment. Confirmation of Payee can help prevent fraudulent payments from being made in the first place. In the UK, the Confirmation of Payee service was developed by Pay.UK which runs the UK’s retail payment systems and is anticipated to commence in March 2020.

Under this scheme, banks in the UK will commence account name checks, also known as confirmation of payee. This added new measure will assist in preventing scams. Currently, consumers are asked to enter the account name when they send money online, but the bank does not check if the account name is correct.

Under the new system, when a consumer enters the account name the bank will undertake a check and advise of the best course of action from three possible outcomes. First, if they use the correct account name, they will receive confirmation that the details match and can proceed with the payment. Second, if they use a similar name to the account holder, they will be provided with the actual name to check. Thirdly, if the customer enters the wrong name for the account holder, they will be told the details do not match and to contact the person or organisation they are trying to pay.

The ACCC strongly recommends that similar initiatives be considered in the Australian market. Where other jurisdictions make it more difficult for scammers, Australian consumers and businesses are at increased risk of being key targets for scammers.

General comments

The ACCC is concerned that the current code in effect excludes transactions initiated by the customer as a result of falling victim to a scammer or fraudster. Even if they were tricked into authorising a transaction unintentionally. We understand that the major banks have different approaches to whether they will consider conduct unauthorised – with some providing refunds to consumers where the consumer authorises another to remote access in to their computer while other banks don’t.

The genesis of the Code was that as banks pushed more people onto electronic banking, risk was moved from the banks, under established banking law, to consumers. The Code was designed to rebalance those risks. Many of today’s scams would not have been possible before the advent of electronic banking and did not exist in the Code’s early days.

The need for an appropriate balance remains. The Code does not take into account the increasingly sophisticated nature of scams, associated consumer behaviour and the growing volume of contact with potential victims. Scams are increasingly hard to distinguish and consumers are tricked into authorising transactions that they would otherwise not authorise.

Similarly, scammers rely on bank systems not verifying incorrect banking details with the account name. We note a mere on screen warning about the importance of entering the correct BSB and account number is not enough. Consumers expect the banks to have sophisticated systems that would detect incorrect BSB and account numbers associated with account names. For example, in business email compromise scams, scammers hack the business and send emails to clients to pay their invoices by using the correct account name of the business but providing the scammer's account numbers hence tricking the clients. We understand that some banks provide some checking to prevent business email compromise scams but a consistent approach that provides better protection is preferred.

Small businesses

The Code protections should extend to small businesses. Scamwatch statistics indicate an increasing prevalence of electronic banking problems facing small business customers.

Australian businesses were hit hard by scammers in 2018 with sophisticated 'business email compromise' scams costing businesses over \$60 million. Again, this would be a vast understatement of losses as most small businesses tend to report scams to their bank and not to us.

Definitions of small business are not standardised within Australia and can differ between regulatory bodies. One of the most used definitions of small business is the Australian Bureau of Statistics (ABS) definition. This defines small businesses as employing 19 or fewer people.

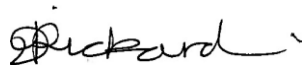
The ACCC and the *Competition and Consumer Act 2010* do not provide a general definition of a small business. However, in terms of business to business unfair contract terms the law provides that unfair contract terms protections apply to small businesses that employs less than 20 people, including casual employees employed on a regular and systematic basis.

Conclusion

While we have been encouraged by the efforts of some financial institutions in recent times in terms of scam prevention initiatives, we are still seeing increasing losses to scams each year and have concerns about the impact on individuals, businesses and the whole economy. We encourage ASIC to consider and explore how the principles that underpin the recent initiatives in the UK might provide better protections for Australians as well as additional certainty and consistency across the financial services sector in dealing with scams.

If you would like to discuss our comments further, please do not hesitate to email Eti Abdulioglu, Assistant Director Consumer Strategies & Engagement Consumer, Small Business & Product Safety Division at CCCSecretariat@acc.gov.au.

Yours sincerely



Delia Rickard
Deputy Chair
Australian Competition and Consumer Commission