Government of **Western Australia**
Department of **Mines, Industry Regulation and Safety**
Consumer Protection

Our Ref: A38349597 / CP01884/2011

09 July 2021

Enquiries:

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

Dear Sir/Madam

REVIEW OF THE EPAYMENTS CODE

The Department of Mines, Industry Regulation and Safety – Consumer Protection Division (Consumer Protection) provides the following submission to the Review of the ePayments Code (the Code) (Consultation Paper 341).

Consumer Protection operates WA ScamNet (www.scamnet.wa.gov.au) through which consumers are forewarned about scams and are provided with the opportunity to report scams. WA ScamNet monitors scam activity and reports and provides guidance to consumers through public awareness campaigns about current scam trends.

In the course of this work, WA ScamNet often identifies regulations, laws and codes of practice that could be improved to offer better protections to ensure Australians are better protected from scams.

This submission addresses the proposed actions categorised as C3 and E1(a):

> *"C3 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."*
>
> *"E1 We propose to adjust the wording of the Code to:*
>
> *a) clarify that the unauthorised transactions provisions only apply 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 a misunderstanding or falling victim to a scam)(sic); ..."*

Consumer Protection strongly submits that these changes, which explicitly exclude from the protection of the Code payments made as a result of a scam, are detrimental to consumers and to the financial sector at large. These proposed changes are effectively taking the Code in the wrong direction and are reducing consumers' ability to seek redress for scams. This could ultimately contribute to a decline in consumer confidence in the financial sector.

Scam Reports

Criminal activity in the form of scams continue to cause significant detriment to Australians. Financial losses through scams impacts the Australian economy as money otherwise intended for legitimate purchases is being directed into the bank accounts of scammers. Given the rise in cyber-attacks on businesses and consumers alike, the disruption of scams continues to be a high priority for Consumer Protection.

In the period 2018-2020, WA ScamNet received scam reports totalling financial losses of over $34 million. In 2021 to date, total losses already exceed $6 million. While this level of financial losses is significant, the emotional damage that victims of scams suffer is unquantifiable in dollar terms. Consumer Protection has had contact with many victims who have developed ill health, depression and other symptoms of trauma as a result of falling victim to a scam.

Given these substantial losses, financial service providers need to have greater obligations to provide better detection practices and preventative measures to assist customers to protect themselves from scams.

Types of scams

ScamNet receives reports regarding a multitude of different types of scams which are constantly evolving as criminals become increasingly sophisticated and frequently changing their approach. The Australian Competition and Consumer Commission's ScamWatch Division (ScamWatch) collaborates with numerous government agencies, including WA ScamNet, as well as banks and payment platforms, to publish an annual report titled *Targeting Scams*, which compiles statistics to provide an overview of scam trends impacting Australian consumers and businesses. The *Targeting Scams* report found that investment scams were the largest contributor to financial loss caused by scams in 2020, totalling $328 million, followed by romance scams with $131 million and business email compromise scams (payment redirection scams) with $128 million.

One thing these different types of scams have in common is that one party believes they are transferring money to a legitimate party but in fact the receiving party will instead be impersonating a party known to the sender. Once the funds are deposited into the scammer's account, the funds are often moved quickly to a multitude of other accounts, making it almost impossible to recover the victim's money.

The frequency of these scams continues to be on the rise and generate significant media attention. In fact, while in the process of preparing this submission, the ABC reported on the experiences of an ex IT professional, Mr Tony Papagiannopoulos, who fell victim to an investment scam totalling $200,000. Mr Papagiannopoulos believed he was investing in bonds with JP Morgan after substantial research online and even attempted to make contact through legitimate JP Morgan phone numbers at one stage, however it was not until his wife received a call from the same number which his phone categorised as a 'suspected scam' did he realise what had occurred. Upon this realisation, Mr Papagiannopoulos contacted both the sending and receiving bank, but unfortunately they were only successful in recovering $114,000.

Consumer Protection has seen a substantial increase in the amount of payment redirection scams across a number of high value industries including real estate and motor vehicles. These occur when criminals scam an individual or a business into paying funds into the scammer's bank account by intercepting emails or sending fake emails from a spoofed email address to consumers, providing them with alternate bank account details.

During 2020, 31 people reported total losses of approximately $739,000 to payment redirection scams in Western Australia. As of March 2021, 16 victims have already lost $500,700. One of these examples involved the granddaughter of a 102 year old woman who believed she was transferring $375,000 to an aged care facility for her grandmother's accommodation but was sent fraudulent account details by scammers in an email. Another example involved a consumer purchasing a Tesla online. Scammers intercepted the email and edited the PDF invoice to change the bank account. The consumer lost $73,000 in that scam.

Current Practice – Australian Banks

As the Australian banks have pushed consumers towards electronic banking in an effort to reduce their operating costs, the risk of financial loss through payment redirection scams has transferred disproportionately to consumers. The scams of today are considerably more advanced and sophisticated than in previous years, and have been made possible by the advent of electronic banking.

Banks in Australia will only check the BSB and account number. They do not currently match the account number with the account name, despite the information and the technology being available for them to do so.

The Code merely requires that banks place a warning notice on the internet banking platform to warn consumers to carefully check the account number to ensure it is correct as the monies will be paid into that account. This does not help with payment redirection scams, as the consumer is entering the account number correctly; it just happens to be the account number for the scammer's account. In this manner, the Code falls significantly short of the standard of other similar codes around the world and does not afford protection to consumers that fall prey to payment redirection scams.

Alternative proposals – Contingent Reimbursement Model and Confirmation of Payee

Consumer Protection notes at paragraph 63 of the Consultation Paper it states:

> *We do not think the Code is an ideal place to set rules for preventing and responding to scams. We think that the issue of whether to extend the Code to deal with industry's response to scams should be considered as part of the process of making the Code mandatory. We do not believe we can deal appropriately with subscribers' response to scams in a voluntary Code.*

Consumer Protection respectfully disagrees and points to the Contingent Reimbursement Model (CRM) Code for Authorised Push Payment Scams as an example of a voluntary code achieving relatively strong protections for victims of scams by incentivising financial institutions to protect their consumers by implementing procedures to detect and prevent scams and also to prevent their accounts being used to launder the proceeds of these scams.

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

The *Contingent Reimbursement Model (CRM) Code for Authorised Push Payment Scams* (the CRM code) was introduced in the United Kingdom (UK) in May 2019. This was in response to losses of over £300 million to authorised push payment (APP) fraud in the UK. APP fraud is referring to scams where customers are misled into authorising a payment to an account that they believe belongs to a legitimate payee, but actually is controlled by a criminal. This is what we refer to in Western Australia as a payment redirection scam.

The CRM code, while voluntary, means there is a no blame model for scams and a fair system of redress is available to consumers. It places the onus on the banks to actively identify and warn customers about scams. The CRM code considers a combination of the individual circumstances of the victim and the scam itself, ultimately weighing this against whether or not it was reasonable for the consumer to have protected themselves. If it was not reasonable, for example, if the consumer is from a vulnerable group, or the scam was highly sophisticated, the consumer should be able to recover the funds.

Most importantly, the CRM code states that if a customer has been the victim of an APP scam (or payment redirection scam), the provider should reimburse the customer. There are some exceptions where the consumer may not be entitled to reimbursement, for example, if the consumer has ignored warnings from the provider.

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.

By contrast, in Australia these types of scams do not fall within the protections afforded under the 'unauthorised transactions' rules of the Code. Consumers are usually unable to obtain redress because they are considered to have authorised the transaction even though they were misled.

On this basis, Consumer Protection strongly recommends the adoption of similar provisions as the CRM for payment redirection scams in the Code. This will provide a strong mechanism for redress for consumers that have been misled into depositing funds into an incorrect account. As cyber risks increase, the adoption of similar provisions in the Code will improve the resilience of Australia's financial institutions and digital payment organisations to the growing risk of online threats and scams.

Payee/Account Name Checks

Consumer Protection further notes that it is proposed at C4 of the Consultation Paper to require financial institutions to provide additional important information in the on-screen warning about mistaken internet payments and to encourage further uptake of the PayID system in lieu of implementing a "confirmation of payee" service in Australia. Again, Consumer Protection respectfully disagrees with this proposal.

Additional information in the on-screen warning about mistaken internet payments will be of negligible benefit in protecting consumers against scams. The proposed "call to action" to the consumer to check that the Bank State Branch (BSB) and account number are correct is unlikely to add value. As noted above, the scam victim is entering the BSB and account number correctly; it just happens to be the account number for the scammer's account.

At clause 82 of the Consultation Paper it states:

> *We think enhanced consumer and business familiarity with, and use of, the PayID service—a purpose built account name and account identifier matching service—will present a number of important 'roadblocks' for scammers who currently take advantage of the shortcomings of the BECS arrangements in the context of the electronic payment behaviours of today's consumers and businesses.*

Consumer Protection does not support this approach. It places responsibility for creating a PayID on the individual consumer, rather than the financial institutions taking any responsibility for making this happen. This has resulted in a somewhat sluggish uptake of the system. By contrast, the "confirmation of payee" system places the responsibility on the financial institutions to implement the required changes, which in Consumer Protection's view is where the responsibility should vest. It would also accord with what many consumers believe is happening at present – that financial institutions are matching the account name with the account number.

The software to make the comparison between the account name and account number is already available; it is currently being used in the UK. This "confirmation of payee" system would make an immediate positive impact in preventing payment redirection scams with minimal regulatory cost to financial institutions. It would not allow an environment that is rich for payment redirection scams to continue to thrive while the community waits for increased uptake of the PayID system.

The "confirmation of payee" system is simple and would work well with vulnerable consumers. Currently in the UK, when attempting to complete an electronic funds transfer, consumers will receive one of four outcomes when they enter both the account name and number:

1. Yes – the name and account type you supplied matches the details on the account – proceed with payment.
2. No – the name does not match the name held on the account. Please check with the payee.
3. No – the name is a close match, the name on the account is 'Joe Bloggs'. Please check with the payee.
4. Unavailable – it has not been able to check the name because of a timeout, account does not exist, and account is not supported for confirmation of payee etc.

For the vulnerable consumer, a response of 2 or 3 above would likely be sufficient to alert them to seek assistance and avoid making a payment to a scammer.

Implementing the UK's "confirmation of payee" system in Australia would be a significant and better step in preventing scams utilising electronic banking. Consumer Protection strongly recommends that this initiative be considered for implementation in the Australian market. As other major jurisdictions are making it more difficult for scammers, Australian consumers risk further exposure as targets for scammers.

Conclusion

While some financial institutions have been making efforts to prevent scams, Consumer Protection is still seeing an increasing number of reports with growing losses from consumers who are falling victim to payment redirection scams. The proposed changes in C3 and E1(a) of the Consultation Paper are a step in the wrong direction, in terms of providing better protection from scams.

We encourage ASIC to consider the initiatives pioneered in the UK and how these initiatives may assist in reducing the risk of payment redirection scams in Australia. Consumer Protection strongly believes these measures would establish consistency across the financial sector in dealing with scams and provide effective models for both prevention and redress for Australian victims of scams.

If you would like to discuss Consumer Protection's comments further, please contact , A/Director Retail and Services, on or via email to

Yours sincerely

COMMISSIONER FOR CONSUMER PROTECTION