WEstjustice

2 July 2021

Australian Security and Investments Commission
GPO Box 9827
Brisbane
QLD 4001

By email: epaymentscode@asic.gov.au

Dear Madam/Sir

RE: Submission to Consultation Paper 341 (Review of the ePayments Code: Further consultation)

1. WEstjustice appreciates the opportunity to contribute to the review of the ePayments Code.

2. WEstjustice is a generalist community legal centre operating in the Western Suburbs of Melbourne. Our practice provides specialised assistance in consumer and civil law matters to recently arrived individuals, households and families, including those from a refugee and/or culturally and linguistically diverse (CALD) backgrounds.

3. Accordingly, we approach the submission through the lens of what we see as particular risks for this group involving unauthorised or mistaken transactions. We also confine our response to those areas of the paper we consider would have the biggest effect on that client group.

WEstjustice's clients and their risk factors

4. The type of issues which can involve the ePayments Code that our clients seek help or assistance on encompass three main areas:
   - Unauthorised transactions arising from fraud or identity theft;
   - Mistaken transactions;
   - Transactions made which are induced by a scam

5. We note ASIC's view that the Code is not designed to deal with transactions authorised by a consumer but that involve electronic transfers to an individual or organisation who is in some way deceiving them or misleading them. However, consumers who have been the victims of scams are increasingly prevalent in our casework.

6. In general, the clients who present with these issues in our casework:

   - Are refugees or otherwise new to very new arrivals in Australia (may have less familiarity with Australian agencies and institutions and be unable to differentiate legitimate ones from scammers or fraudsters);
   - Are from low income or Centrelink reliant households (the impact of money lost due to fraud or a scam will be more immediate in terms of impact on essential and ongoing costs of living);
   - Have low English language skills (may have more difficulty navigating online banking messages and correspondence, and identifying signs of fraud or scam attempts);
   - Have low technological literacy (more difficulty navigating online environments, including online banking, and at greater risk of fraud or scam attempts that occur in the online environment).

7. WEstjustice's general view is that an effective ePayments Code should act as a safety net for particularly at-risk customers, both in terms of preventative measures and mitigating the harm of sudden and unexpected financial loss.

Proposals C3 and E1 – Narrowing consumer rights in relation to scam events

8. WEstjustice strongly opposes these proposals, which would further narrow the already limited ability for at-risk consumers to recover payments made to scammers in the event of a 'mistaken internet payment' (C3) or an 'unauthorised transaction' (E1).

9. Scams are not homogenous, and may involve varying degrees of deception depending how sophisticated (and targeted) the scammer is. There is not a unified Australian definition under legislation for a 'scam'. We note that a scammer may:

   - Provide doctored ID or bank statements, leading to a mistaken payment or 'payment redirection' despite a sender taking what would otherwise be considered to be reasonable precautions;
   - May proactively influence and manipulate a customer and conceal their true nature, such that a transaction could arguably be said to be unauthorised.

10. ASIC states at paragraph 63 of the Paper that it does not consider the Code "an ideal place to set rules for preventing and responding to scams" and that whether the Code be modified is a subsequent question that should be addressed as part of a future discussion about making the Code mandatory.

11. The Paper supports the view (which WEstjustice shares) that consumers should not suffer losses through mistaken internet payments and scams as a result of deficiencies in the way payment instruction and processing systems have been designed. However, it notes that the introduction of certain automatic measures that would improve these systems (such as implementing a Confirmation of Payee service) requires a policy position from the government.

12. A narrowing of the application of the 'mistaken internet payment' or unauthorised transaction provisions of the Code would reduce consumer protections in cases where we consider our clients genuinely made mistaken or unauthorised transactions at great personal and financial harm. This is particularly the case where there is no proposed or confirmed date by which any expansion of the Code or parallel Code for scams would be created, and no set date for the rollout of additional protections when an e-payment is to be processed.

13. For the avoidance of doubt, WEstjustice does not consider that the ePayments Code serves as a comprehensive model to address situations where clients are the victims of scams, and consider that a significant regulatory gap remains in this area. However, restricting the ePayments Code, without providing a comprehensive and binding framework for addressing victims of scams elsewhere (be it via an amended Code or elsewhere) at this time only makes that gap more harmful. This is especially the case as scammers become more sophisticated and have furthered their reach in the ePayments space in an unprecedented manner.[1]

14. Until a suitable alternative protection is provided, the ePayments Code is the only means of protection and possibly restitution available to our at-risk clients who have fallen victim to these scams.

Recommendation 1: The definitions of 'mistaken internet payment' and 'unauthorised transaction' under the Code should not be narrowed in the absence of a dedicated section of the Code (or separate Code) dedicated to scams.

Proposal C4 – Providing specific information by way of on-screen warning about mistaken Internet payments

15. WEstjustice strongly supports a proposal that an on-screen warning:
    - Contain a 'call to action' for a consumer to check that the BSB and account details of a recipient are correct;

[1] See further Australian Competition and Consumer Commission, *Targeting Scams: Report of 2020* (2020) which reported cyber scams increased significantly during the pandemic period.

- In plain English, include wording outlining the effect of a mistaken transaction.

16. We consider that precise wording or some form of benchmark mandatory language is preferable to flexibility as to an on-screen warning's content.

17. However, having mind to our client base, we consider that important wording of this nature be developed in consultation with and using the expertise of culturally and linguistically diverse users/communities so that industry has confidence that wording would be understood by users with lower levels of English.

18. We note that as a matter of efficiency, such consultation could also encompass guidance for any other ASIC codes or regulatory guides which presently mandate the use of plain English for documents or communication.

Recommendation 2: Precise wording or mandatory language be used for on-screen warnings, and this be evaluated before use with culturally and linguistically diverse users.

Proposal C2(d) – Non-cooperation by a receiving ADI not relevant to whether sending ADI has complied.

19. At paragraph 57 of the Paper, ASIC notes that the Mistaken Internet Payment framework depends on cooperation by both a sending and receiving ADI. If non-cooperation occurs on the part of a receiving ADI, it notes the sending ADI has little if any ability to ensure return of the funds.

20. ASIC further notes that it has considered specifying that AFCA's rules may enable determinations against a receiving ADI for failures to cooperate, but ultimately decided against this as there are not contractual obligations between the receiving ADI and the customer who made the mistaken internet payment.

21. WEstjustice notes that elsewhere, AFCA's rules allow for complaints arising other than in a strict contractual relationship, including complainants who may have a right or benefit under a policy of insurance despite not being the policyholder, a claim by a complainant under another person's motor vehicle insurance product in the event of property damage or non-financial loss, and breaches of the Privacy Act or the Consumer Data Framework.

22. It is unclear why, given an expectation that ADI's should co-operate in the context of a Code they have agreed to participate in, a receiving ADI that does not engage should be able to do so without any consequence. The lack of any remedy to a

customer in this instance could mean that transactions that fall squarely within the Code's ambit, and which could and should be promptly investigated, are never recovered.

Recommendation 3: A change be made to the AFCA rules stipulating that customers may bring an AFCA complaint against a receiving ADI in the event of a mistaken payment under the Code.

Proposal C1 – Clarification about partial refunds and examples of reasonable endeavours to retrieve funds

23. We support the proposal to clarify that a consumer can retrieve at least a portion of a mistaken internet payment.

24. WEstjustice are not aware of any matters arising from our present casework in which an ADI has taken a highly literal construction of the processes at clauses 28-30 and refused to assist in retrieving a smaller or partial amount. Nevertheless we consider this clarification important. Our clients will face hardship with utilities, rent and servicing other loans in the event of losing money to a mistaken transaction. In these circumstances, even a little goes a long way.

25. We believe that further consultation should be undertaken about clarifying reasonable endeavours a receiving ADI should take to retrieve mistaken internet payments. This is a welcome but significant amendment to the Code which, while non-exhaustive, will certainly set the tenor of what expectations will be placed on an ADI in these instances.

Recommendation 4: ASIC should clarify that processes under the Code to retrieve money in a recipient's account apply where only a portion of the funds is available in a recipient's account.

Recommendation 5: ASIC should conduct further consultation on the list of reasonable endeavours a receiving ADI is expected to undertake to retrieve a consumer's funds.

The Need for A Wider Review Project

26. The Consultation Paper identifies a range of significant potential developments to the Code which are considered outside the ambit of the review, including whether the Code becomes mandatory, the implementation of additional positive obligations on

payment instruction and processing systems, and the development of a comprehensive set of provisions (inside the Code or in another code) on scams.

27. We believe a wider review that allows stakeholders to contribute and inform policy would be the most effective way to develop effective and futureproofed regulation of ePayments and scams. We favour this over a piecemeal approach, particularly where this risks reducing some protections for our clients (as outlined at Recommendation 1 above).

Recommendation 6: Any substantial changes to the Code should be delayed to allow a comprehensive review of ePayments and scam regulation to take place.

28. We would welcome the opportunity to discuss this submission further. Please contact WEstjustice on (03) 9749 7720, or email either ( ) or ( ) if you have enquiries about our work in this area.

Yours sincerely,

CEO
WEstjustice