FRAUD ADVISORY PANEL

FRAUD ADVISORY PANEL REPRESENTATION 08/18

RESPONSE TO THE AUTHORISED PUSH PAYMENT SCAMS STEERING GROUP ON A DRAFT CONTINGENT REIMBURSEMENT MODEL CODE PUBLISHED ON 28 SEPTEMBER 2018

The Fraud Advisory Panel welcomes the opportunity to comment on the consultation published by the Authorised Push Payment Scams Steering Group (the 'Steering Group') on the draft contingent reimbursement model code on 28 September 2018, a copy of which is available from this link.

This response of 15 November 2018 reflects consultation with the Fraud Advisory Panel's board of trustees and interested members who are counter-fraud professionals and financial crime specialists from all sectors. We are happy to discuss any aspect of our comments and to take part in all further consultations on the issue of authorised push payment fraud.

CONTENTS **PARAGRAPHS**

The Fraud Advisory Panel (the 'Panel') is the UK's leading anti-fraud charity.

Established in 1998 we bring together counter fraud professionals to improve fraud resilience across society and around the world.

We provide practical support to almost 300 corporate and individual members drawn from the public, private and voluntary sectors and many different professions. All are united by a common concern about fraud and a shared determination to do something about it.

For more information, please contact info@fraudadvisorypanel.org

www.fraudadvisorypanel.org

INTRODUCTION

1. We believe that there need to be better incentives for firms and customers alike to reduce APP fraud insofar as possible and to make it harder for fraudsters to succeed. Our goal should be to create a realistic and practical solution to a growing and costly problem that is in the interests of honest customers and firms alike.

2. As part of this, firms should have adequate safeguards to prevent fraudsters from setting up, controlling or manipulating bank accounts. They should also have better procedures to detect fraudulent accounts quickly and take rapid action to block them. This should include: keeping their fraud departments open 24 hours; empowering fraud departments to share information with other firms involved; and providing clear signposting to customers online, in branch and on automated phone systems for reporting suspected fraud and to facilitate quick action. Firms also need to give customers the knowledge they need (using a variety of delivery channels) to spot the warning signs and protect themselves.

THE CURRENT CONSULTATION

3. Generally speaking, we welcome the creation of an industry good practice code for the reimbursement of APP fraud victims. We believe that this is a positive step towards ensuring that victims are treated fairly and consistently. However, like any voluntary code, it lacks enforcement 'teeth' for firms that do not follow it which could be detrimental to other firms and customers alike.

4. Therefore we hope that all firms will choose to adopt the code as soon as possible as a matter of industry-wide good practice. Every firm should be required to tell potential and actual customers whether they are signed-up to the code so that customers can make informed choices about their banking service providers. In addition, the industry should take steps to inform the public more generally about the code and which firms have committed themselves to it as a means of fostering public awareness and confidence (of both the code and the ways to prevent APP fraud).

5. Consumer guidance in this area is key and it should be simply written to aid understanding and be available in a range of languages. However, we remain concerned about the continued use of the word 'scams' to describe fraud which we consider trivialises the crime and its harmful effects on victims. Our use of language in this area is crucial to ensuring that positive initiatives like this are given the priority they deserve.

6. We note that the code does not apply to international payments or payments made in other currencies and recognise that there are significant jurisdictional challenges in it doing so. However we question whether this will simply displace the focus of fraudsters' endeavours to these types of payments, so we encourage the sector and regulators to develop effective preventative measures (such as additional warnings and advice to customers about the risks associated with foreign payments and currencies) to stop this occurring insofar as possible.

RESPONSES TO SPECIFIC QUESTIONS

A. THE DRAFT CODE

Q1: Do you agree with the standards set out in the Standards for Firms?

7. In principle we agree with the draft standards SF1 and SF2 as set out in the draft code. However we believe that these should be reviewed within a reasonable time period of industry adoption to assess whether they are operating as intended and fit for purpose and then on a set periodic basis thereafter. In addition, the current proposals address only microenterprises, charities and individual customers; we believe the impact on corporate entity customers should also be considered.

8. We are particularly supportive of the minimum criteria for effective customer warnings (that they should be understandable, clear, impactful, timely and specific) and the constituent element that the customer is given clear guidance about the action they should take to avoid the risk of falling victim to an APP fraud. This latter point has been missing from much customer advice to date. Many firms simply provide warnings stating that once a payment has been authorised it cannot be returned and say nothing about the need to independently verify bank account details etc. Any actions suggested to customers must be practical and simply expressed to be truly effective preventative tools and need to be displayed at appropriate points in the customer's payment journey.

9. In our responses to previous consultations on this issue, we have suggested that firms may wish to consider compelling customers to take a five-minute interactive training session (or to watch a short video) every six months or so which explains APP risks, the common ways fraudsters try to trick victims, and the most important things they need to do to prevent it. This could be done, for instance, by building it in as a step for certain types or sizes of online transactions or when setting up or amending a payee. Consideration should also be given to providing advice at key financial milestones whereby vulnerability may be heightened, for example, during the mortgage approval process before a deposit is paid, when an unusually large lump sum (from a pension or inheritance) is deposited or when a loan has been approved. This would enable firms to show in a consistent and uniform approach to awareness and education.

10. The Standards for Firms state that '*If firms fail to meet these standards, they may be responsible for meeting the cost of reimbursing…*'. More consideration should be given to how this will be determined and by whom: will it be the sending firm, the receiving firm, an independent body, or a panel of these? Delays could be caused by lengthy investigations into whether the firms involved have met the standards or not. The definition of failing to meet could also vary significantly with the size and sophistication of the firms and customers involved.

11. The confirmation of payee requirement is an important part of combating APP fraud. However, paragraph 3.42 of the consultation paper states that the steering group does not want confirmation of payee to interrupt legitimate payment journeys unnecessarily. This may not be possible given that matching the payee's name to the account details may produce false positives which will necessitate investigation. This will take time and could cause delays to payments given that these checks are an additional step in the payment process which does not currently exist.

12. Furthermore paragraph 3.45 states that '*firms are encouraged to take steps to delay payments or freeze funds so they can make investigations where they are concerned about APP scams*.' This contradicts paragraph 3.42 in that firms will need additional time when payee name and account details do not match. This and other red flags need to be investigated. More consideration is needed on how these new requirements may place additional burden on firms and result in delays to payment journeys whilst investigations are performed.

Q2. We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims.

13. We believe that it should be possible to mitigate most unintended consequences in this regard through independent review of the adequacy of the effective warnings provided to the customer and verification of the customer's compliance with these warnings by way of complaint to the Financial Ombudsman Service (FOS). We reiterate our earlier points that effective warnings should include practical actions that customers can perform to confirm that a payee or payment is genuine before proceeding with the payment and that customers should be compelled to complete periodic online training.

14. One scenario which might prove much more problematic is R2(1)(e) whereby a microenterprise or charity does not follow its own internal procedures for approval of payments, particularly if that entity has:
    a. no formally documented procedures, and/or
    b. been the victim of a rogue employee, and/or
    c. had its email system compromised or credentials stolen by hackers.

    It should be borne in mind that many microenterprises consist of a single individual, who is unlikely to be in a position to take more security measures than a retail customer.

Q3. We welcome views on how provisions R2(1)(a) and (b) might apply in a scenario where none of the parties have met their levels of care.

15. This question is difficult to understand and interpret. However if our understanding is correct, R2(1) sets out the criteria under which a firm may choose not to reimburse a victim. However in order to establish whether none of the parties involved have met their levels of care we believe you also need to take into account R2(2) which requires firms to consider whether they have meet the Standards for Firms or not.

16. It is our view that once such an assessment has been made by the firm, an independent determination can then be made as to which party has been the most competent/negligent and a proportionate reimbursement model applied (for example, an apportionment of 2/3s). Difficulty may arise if one of the firms involved is not a signatory to the voluntary code. An industry-wide protocol may be needed for the disclosure of confidential customer information (which may include the owner of the fraudulent account) to the independent third party.

17. If independent third parties are to be used to determine whether firms failed to meet the standards, consideration should be given as the background and experience required of those parties and whether their decisions will be binding.

Q4. Do you agree with the steps customers should take to protect themselves?

18. Yes. We agree with the steps that customers should take to protect themselves.

19. However we also note that most victims of APP frauds genuinely believe that they are making a payment to a legitimate payee, otherwise they would not be making the payment in the first place. The sophistication of many such frauds means that it can be very difficult for the average person – however carefully they manage their affairs – to distinguish between the genuine and the criminal, and this is why the awareness-raising efforts of firms is so important. Frontline staff could also benefit from enhanced training in this regard to ensure that they ask customers the right questions (particularly in branch) when payments are being requested (for example, 'have you checked the bank account details are correct by …'). We understand that some firms are already doing this.

20. We agree that where customers have caused deliberate obstruction to firms investigating APP frauds or provided false information then firms can decide not to reimburse them (R2(1)(f). However in making such an assessment, firms will need to take into account extenuating factors such as whether the victim has been coached by the fraudster (impersonation frauds) or simply forgotten important details because of the stress caused by the victimisation itself or other circumstances. These situations should not be legitimate reasons for firms not to reimburse the customer.

21. Further consideration should also be given to how firms will go about proving the criteria set out in R2(1)(c),(d),(e) and (g). There may be limited evidence available to prove or disprove the facts around whether a customer, for example, '*recklessly shared access to their personal security credentials…*'. As noted above, consideration should be given to who will do these investigations and make decisions about negligence. These investigations could prove to be very time-consuming and costly for firms, especially if they have to engage with independent third parties or create new teams to review reimbursement claims and respond to disputes between firms.

Q5. Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

22. We agree that vulnerable customers should receive extra help to protect themselves and be assessed on a case-by-case basis to determine whether their personal circumstances indicate that they are vulnerable and should be eligible for reimbursement, regardless of whether the customer has been identified as vulnerable prior to the victimisation.

23. One unintended consequence of this approach could be that firms exit customers who are vulnerable and/or present a greater risk of causing loss to the firm as a result of falling victim to APP fraud and other frauds.

24. We recommend that if the code adopts BSI PAS 17271 'Protecting customers from financial harm as a result of fraud or financial abuse: code of practice' as a standard then the standard should be made publicly and freely available to customers for transparency and accountability purposes on a similar basis to the former PAS 1998:2008 'Whistleblowing arrangements: code of practice' (now withdrawn). Customers should also be signposted to it.

25. We also believe that firms could benefit from the experiences of the Action Fraud 'National Economic Crime Victim Care Unit' in respect of assessing vulnerability.

Q6. Do you agree with the timeframe for notifying customers on the reimbursement decision?

26. We believe that the proposed timeframe for notifying customers on reimbursement decisions (within 15 business days or 35 business days in exceptional cases) is a significant improvement on the current situation. Further guidance is needed on what constitutes an exceptional case.

Q7. Please provide feedback on the measures and tools in this Annex, and whether there are any other measures or tools that should be included?

27. Other good consumer awareness and education tools include the GetSafeOnline website and the Metropolitan Police Service's 'The Little Book of Big Scams' and 'The Little Book of Cyber Scams'. For microenterprises and charities the National Cyber Security Centre has published the following: '10 Steps to Cyber Security', Cyber Security: Small Charity Guide', and 'Cyber Security: Small Business Guide'.

28. Another measure could be to ask customers to complete a short checklist when amending an existing payee or setting up a new one in branch or online to confirm that they have taken adequate precautions.

B. OUTSTANDING ISSUES

Q8. Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

29. Yes, in principle this seems to be the correct approach but it will depend to some extent on the final funding model adopted.

Q9. Do you agree that the sending firms should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

30. Yes.

Q10. What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?

31. We reserve our opinion on the funding options outlined in paragraph 4.6 until such time as further details are available. We hope that these will be the subject of a separate consultation.

32. We note that any new requirements (voluntary or otherwise) on customers to obtain insurance policies and/or pay additional charges on certain transactions may result in some customers looking for cheaper (and probably less regulated) ways to make such payments, for example,

cryptocurrencies and other higher risk transfer methods which may simply move the risks elsewhere.

33. In addition to the Criminal Injuries Compensation Scheme (CICS) another existing model that might merit consideration is the Motor Insurers' Bureau (MIB) which is the mechanism through which compensation is provided for victims of motor vehicle accidents caused by uninsured/untraced drivers.

34. In order to ensure the longevity of any funding model introduced it may be necessary to set a maximum value on reimbursement as per the CICS.

Q11. How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

35. Firms will need to document evidence of the steps taken. Customers will need to show that they contacted the firm as soon as possible after they realised they had been defrauded and followed the advice they had been given. This may also include details of any checks they did on the payee before making the payment.

Q12. Do you agree with the issues the evidential approach working group will consider?

36. Yes. We agree that clear guidance is needed on the type of evidence which will be expected to be created and maintained when an APP fraud occurs, for both the firms and the customer. This will lessen the likelihood that there will not be enough evidence to complete a balanced investigation. Customers may feel at a disadvantage when dealing with their banks given the firms will be more sophisticated in producing evidence and defending their compliance with these standards.

Q13. Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

37. No.

Q14. How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

38. Some customers may need to waive their privacy in order to demonstrate vulnerability. This would be a decision for the individual customer or an appropriate other person. A customer could be given a standard checklist to voluntarily supply relevant information to assist with the assessment process.

Q15. Please provide views on which body would be appropriate to govern the code?

39. We believe that the Payment Services Regulator is the most appropriate body to govern the code.

40. To foster public confidence and assurance in the integrity, independence and impartiality of the code it should not be governed by a body that represents the interests of a specific group of stakeholders such as financial services firms (for example, UK Finance) or consumers.

Q16. Do you have any feedback on how changes to the code should be made?

41. We agree that changes to the code should be permitted on an ad hoc basis (especially in response to changes to APP fraud typologies and findings from disputes between firms). These changes must be subject to an open, rigorous and transparent change process.

42. We also agree that the code should be reviewed periodically with the first one conducted a year after the code is finalised and then every three years thereafter. Reviews should be subject to wide public consultation supplemented by proactive engagement with key stakeholders where appropriate.

Q17. Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

43. Yes.

Q18. Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the Code?

44. Further consideration should be given to how these principles are currently operating to deal with disputes and whether there have been any issues in satisfactorily resolving disputes. We note that these principles are also voluntary.

Q19. What issues or risks do we need to consider when designing a dispute mechanism?

45. As noted above, consideration should be given to the evidential standards that would need to be followed to prove whether the standards for firms were met. Consideration should be given to who will adjudicate these disputes and whether they need to be independent from the firms. Customers should be given clear options on how they can appeal when the dispute is not satisfactorily resolved, in a reasonable time period.

C. ADDITIONAL QUESTIONS

Q20. What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

46. We hope that the introduction of the code will have a positive impact on actual and potential victims of APP fraud by reducing the chances of falling victim in the first place (because of better awareness and safeguards) and providing reimbursement (where appropriate) where they do.

47. The main negative impact will be the potential de-risking of certain types of customer (for example, who might be identified as more at risk of becoming money mules) by firms. Appropriate safeguards will be needed to address this. It is our opinion that firms which have confidence in the adequacy of their account opening procedures and effective warnings shouldn’t need to de-risk.

Q21. What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

48. Firms that do not become a voluntary party to the code, who do not follow the prescribed standards, or who close victim accounts as part of de-risking processes, could suffer loss of customer confidence and reputational damage.

Q22. Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?

49. It is likely that there will be an initial increase in the number APP frauds reported to firms because of greater awareness of the standards. However as long as the principles of the code are adhered to consistently these should reduce soon thereafter.

50. There may also be increased costs to customers and/or firms depending upon the final funding model.

51. Finally, there is a strong likelihood that APP frauds will be displaced elsewhere such as international and/or foreign currency payments, and vulnerable victims.

Q23. How should the effectiveness of the code be measured?

52. Effectiveness of the code should be measured by the reduction in the volume and value of successful APP frauds reported to firms.