Financial Services Consumer Panel
AN INDEPENDENT VOICE FOR CONSUMERS OF FINANCIAL SERVICES

Telephone: 020 7066 9346
Email: enquiries@fs-cp.org.uk

APP Scams Steering Group Consultation
c/o Payments Systems Regulator
12 Endeavour Square
Stratford
London E20 1JN

13 November 2018

By email: app-scam-pso-project@psr.org.uk

Dear Sir / Madam

Financial Services Consumer Panel response to the APP Scams Steering Group Draft Contingent Reimbursement Model Code Consultation Paper

The Financial Services Consumer Panel is an independent statutory body. We represent the interests of individual and small business consumers in the development of policy and regulation of financial services in the UK.

The Panel welcomes the opportunity to respond to the APP Scams Steering Group Draft Contingent Reimbursement Model Code Consultation Paper. Our main points are:

- Everyone is vulnerable to fraud, as the consultation paper makes clear. Although some people have more capacity to protect themselves than others, a division of customers into vulnerable and non-vulnerable will not work in practice. The Code should make clear that everyone is vulnerable and all customers should receive protection.
- The Code should explicitly address the risk of APP fraud to SMEs, and confirm that it applies to SMEs.
- There should be a presumption that the receiving bank is at fault where there has been an APP scam.
- Consumers should be reimbursed if they are victims of an APP fraud unless they have been grossly negligent. This is the standard applied to card payments and it should apply to faster payments as well.

The Panel's responses to the questions posed in the consultation document are set out below.

Yours faithfully,

Sue Lewis
Chair, Financial Services Consumer Panel

ANSWERS TO CONSULTATION QUESTIONS

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

To stop scams, or allow money to be returned to consumers more easily, information needs to flow as quickly as money. The technology exists to enable this, but the current legal and regulatory framework does not permit it. This needs to be carefully considered, and may require intervention from Government to bring it about.

The Panel's comments on the standards are divided between those which apply to 'sending' firms and 'receiving' firms.

For 'sending' firms:

The standards for 'sending' firms look broadly acceptable. However, the Panel has four reservations:

1. All consumers are vulnerable to APP scams. Attempting to identify consumers who are likely to be particularly vulnerable does not make sense.
2. SMEs are also at risk and the Code is silent here. This is a gap which should be addressed.
3. The 'sending' firm is only required to notify the receiving bank if it is a UK bank. While the Code does not cover the actions of a receiving bank in another country, we understand that such contact can result in voluntary and prompt action. The 'sending' firm should be required to notify the receiving bank wherever they are so consumers making international payments receive effective warnings and prompt responses if they have fallen victim to scams.
4. Sending banks should offer customers a 24-hour delay for all payments. Where Payment Service Providers (PSPs) warn customers about an APP scam risk, they should remind them that card payments offer significantly more protection, particularly in relation to chargeback.

For 'receiving' firms:

There should be a presumption that the receiving bank is at fault where there has been an APP scam.

The receiving bank has facilitated a financial crime by allowing the fraudster to open an account, or by failing to detect that an account is being used as a money mule account. Under the present system, the receiving bank has no incentive to detect fraudulent payments as they bear no risk. Under the proposed Code the receiving bank has to take 'reasonable steps' to prevent and respond to APP fraud. This is not clear enough. If the receiving bank fails to detect and prevent fraud, it should be liable for losses suffered by the sending customer. Only then will firms have sufficient incentive to put in place robust fraud prevention systems

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

We find it difficult to envisage circumstances where this might apply.

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

The Panel is unable to envisage situations in which these provisions would apply. If the sending bank and receiving bank have both failed, then whatever happens the customer can't be held liable under R2 (1) (a) and (b) and should receive reimbursement. Where all parties have not met their level of care we would expect the provisions of R2 (2) to apply and firms to reimburse consumers as their acts or omissions have "impeded the Customer's ability to avoid falling victim to the APP fraud".

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

Customers should take reasonable care, but are entitled to expect that the bank will have systems and processes in place to protect them, and to help them recover their funds. We believe that all consumers should be reimbursed unless they have been grossly negligent (i.e. R2 (1)(g) only). This is the standard applied to card payments and we believe it should apply to push payments as well. The other standards should not be assumed to define 'gross negligence'. Gross negligence involves conscious and intentional disregard or care. Ignoring a negative Confirmation of Payee (CoP) response (perhaps because CoP is not sufficiently reliable) may be rational and cannot constitute 'gross negligence'.

Consumers are entitled under PSD2 to share their credentials with authorised third parties. R2 (1)(c) is therefore not relevant to authorised push payment fraud but unauthorised push payment fraud. It should be removed.

There is insufficient detail for R2 (1) (d): "Failing to take reasonable steps to satisfy themselves that a payee was the person the Customer was expecting to pay". It is not clear what exact steps customers are supposed to take beyond using the Confirmation of Payee system once it is operational. If the Code cannot provide absolute clarity on this point (e.g. consumers should speak with the recipient in person to confirm the account details and sort Code in advance of making the payment), then R2 (1) (d) should be removed.

We recommend removing R2 (1) (f) from the Code altogether. Where consumers are coached by fraudsters to 'lie' to their bank, they are caught in the scam and cannot therefore be judged against the provisions in the Code. Consumers who are actively involved in fraud are not covered by the Code in any case.

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?

The consultation document states that all consumers are vulnerable to APP scams. We agree. However, the Code should also make this clear. Identifying consumers who are likely to be particularly vulnerable does not make sense. A momentary distraction like a child crying, problems at work, or a short-term illness all make people particularly vulnerable to APP scams. It is not possible to codify and anticipate these events. This section of the Code, as currently drafted, is not workable in practice. The approach should be to assume that everyone is vulnerable, and protect them accordingly.

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

Yes. However, consumers should be able to go to the Financial Ombudsman Service (FOS) immediately if they are unhappy with the reimbursement decision. Firms should

not be able to delay reimbursement or consumers' access to FOS. The easiest way to accomplish this is for the FCA to define a report of an APP scam as a complaint and to turn on the complaints forwarding rules for all complaints about APP scams so that the sending bank has to pass on the complaint to the receiving bank.

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

Better transaction analytics are likely to be forthcoming if the banks, rather than customers, bear the risk of APP fraud. Banks are more likely to develop analytics to protect themselves than they are to protect their customers.

Confirmation of Payee only provides partial protection, especially where a fraudster sets up an account in a name resembling that of the intended payee. For example, if the payer intends to pay Norman Archer and the fraudster sets up an account in the name of NM Archer, Confirmation of Payee will not return "no match". In addition, Confirmation of Payee which relies on checking firms' names with Companies House does not provide adequate protection since the process for registering a company is simple, and liable to be abused by those perpetrating scams.

Banks should offer all customers payment deferral, not just those they identify as vulnerable. This would be much simpler to administer and at least one High Street bank already does it, so it is technically possible.

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

Yes. We believe they should be reimbursed unless they have been grossly negligent, to bring the protection offered by push payments into line with cards.

Q9 Do you agree that the sending firm 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?

The sending firm has the relationship with the sending customer and it therefore makes sense for them to administer the reimbursement. As we have said above, we think the presumption should be that the receiving bank is liable unless the sending bank has failed to meet the Code's standard of care.

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?

We are strongly opposed to an insurance fund or government sponsored fund. This would create a moral hazard, and sharply reduce the incentive for banks to develop systems to protect themselves and their customers from fraudsters.

Under card scheme rules the cardholder's bank is responsible for reimbursing the customer in the event of fraud. Banks do this as part of the cost of scheme membership because they make money from every card transaction.

Faster Payments are free to individual consumers, although SMEs usually have to pay. Banks do not therefore see them as a revenue stream, but as a cost. In reality, Faster Payments enable banks to cut their operating costs by getting the consumer to do the work rather than bank staff, and by reducing the need for branches to handle payments. Banks prefer that consumers use Faster Payments than write cheques or make transactions in cash. They do not offer alternatives to consumers wishing to make

payments directly from their bank (for instance a slower type of payment). The banks themselves benefit from this. It is therefore in the banks' interest to maintain trust in Faster Payments (and Chaps), as they do with cards.

It would be possible to charge individual customers for making push payments. As lower value payments (say less than £5,000) are rarely attractive to fraudsters the charge could be levied only on payments above the threshold. Consumers already pay for larger payments via CHAPS. Incentivising banks by associating Faster Payments with a revenue stream would help to promote usage, and therefore trust.

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

As we have said above, we believe customers should be reimbursed unless they have been grossly negligent, as with cards. The card schemes have a lot of experience of defining what is and what is not gross negligence.

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

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

Yes. We have no recommendations for other issues.

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

Everyone is vulnerable to fraud. Some people will – in that moment – have more capacity to protect themselves than others. As we have said above, it is not possibly to codify and anticipate who will be vulnerable at the point at which they are scammed. A division of customers into vulnerable and non-vulnerable categories will not work in practice.

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

Pay.UK (formerly the New Payment System Operator) is the obvious body to govern the Code. It is the analogous body to card schemes and should be responsible for taking the lead in ensuring that the payments systems it runs are trustworthy.

The body responsible for governing the Code must have the resources, powers and responsibility to collate or gather data on APP scams, conduct compliance assessments and to share best practice. It should also maintain a register of firms which have signed up to the Code. The governing body would need to have a memorandum of understanding with the FOS and receive all of the FOS decisions made about firms with regard to APP scams and compliance with the Code. We would also expect the FOS to draw the governing body's attention to any systemic issues about how firms were complying with the Code. The governing body should also have the power to name firms which are failing to comply with the Code.

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

Pay.UK should lead and work jointly with consumer groups and UK Finance, with input from the Payment Systems Regulator. These bodies should consult regularly with consumer bodies to discuss the Code's effectiveness or changes and improvements.

The Code also needs proper oversight, monitoring and enforcement. Pay.UK could usefully learn from the Lending Standards Board, or commission their support for auditing individual firm's compliance with the Code.

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

As we have said above, the receiving bank should be presumed to be at fault unless the sending bank has contributed.

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?

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

Consumers affected by APP scams need a clear and simple means of registering a complaint, and they should have to do this only once. Under no circumstances should the consumer have to make separate complaints to both the sending and receiving banks. This would add unnecessary duplication and complexity, and raise the prospect that a consumer seeking redress will be passed back and forth between banks, with neither taking overall responsibility.

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

No comment.

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?

The biggest benefit is that more victims should get their money back.

We anticipate that consumers with less formal means of proving their identity will struggle to open bank accounts, exacerbating financial exclusion. There might also be more forced account closures.

Some consumers may also become irritated or frustrated at the imposition of more friction into payments.

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?

There might be some payment delays (e.g. to solicitors) and processes will need to be adjusted to take account of these.

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

As we state in our answer to Q20, the Code may increase levels of financial exclusion, since consumers with less formal identification documents may struggle to open bank accounts.

Q23 How should the effectiveness of the Code be measured?

Key measures to determine the effectiveness of the Code should be the reduction in the number of APP scams and reduction in the level of losses incurred.

Code signatories should be required to report key statistics to the governance body on a regular basis. The governance body should be responsible for monitoring firms' adherence to the Code, and be able to 'name and shame' firms that do not adhere to the Code. Otherwise, the Code will be of little use, other than to provide some guidance on acceptable practice to the FOS. In cases where consumers do not complain or take their concerns to the FOS, they will be worse off.