Consultation Response to APP Scams Steering Group Draft Contingent Reimbursement Model Code

Dr Steven Murdoch, University College London

Thank you for the opportunity to contribute to this consultation, my response is not confidential and may be published and shared with the Steering Group in full.

The introduction of a Contingent Reimbursement Model is an unconventional approach to consumer protection and the Steering Group have made an admirable attempt at tackling the difficulties this creates when compared to more conventional approaches like the Consumer Rights Act and the protection against unauthorized transaction in the Payment Services Directive. These difficulties particularly result from the complex criteria that fraud victims must meet in order to be reimbursed and from the responsibility for reimbursement to be on parties which have no contractual relationship with the victim, resulting in the need for strict governance over the process and the development of rules for evidence. Some of these difficulties could have been predicted (indeed, I pointed some out in my response to the consultation by the Payment Services Regulator[1]) while others appear to have become apparent only during the course the Steering Group's work.

I will discuss some ways in which these difficulties could be mitigated in my answers the consultation questions. In some cases, these mitigations are not how UK banks conventionally do business, and so the firms may prefer less transparency and less external scrutiny. However, it is important to note that these mitigations follow naturally from the application of the Steering Group's principles when taking into account the banking industry's preference for a Contingent Reimbursement Model.

Firms which do not wish such transparency measures should have the option to adopt a more conventional consumer protection approach by having the sender bank reimburse victims unless they can demonstrate that the victim was complicit in the fraud. Whether the sender bank then makes a claim against other parties regarding the handling of the stolen funds would then be a matter that could be resolved privately within the industry.

Similarly, if matters such as the apportionment of funds for reimbursement cannot be resolved by agreement within the industry then the fall-back position of the Steering Group should be for the sender bank to be liable. Taking this approach allows the sender bank to still obtain reimbursement for the funds should another

[1] https://www.benthamsgaze.org/wp-content/uploads/2018/06/pushpayment_murdoch.pdf

party be at fault. In contrast, a victim without access to legal and technical expertise is in a much weaker position to obtain funds which are due.

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

The code refers to "best practice" but too often this is a euphemism for current practice, and such standards serve to entrench poorly evidenced measures that are selected to minimize compliance costs and shift liability away from the industry. This is risk is exacerbated by the code proposing best practice standards developed by the industry itself.

Instead, as proposed by the Royal Society[2] "competent security and reliability must be based on a rigorous and evidence-based standard of engineering – one that is continually rising based on strong scientific evidence. 'Best practice' should not refer to average practice, nor to a check-box approach, but to an ambitious, state of the art standard for security and reliability, informed by research."

Standards which form part of measures that transfer risk from the industry to the customer, such as referred to in the code which is the subject of consultation, should be developed and assessed independently of the industry. Legislation such as surrounding Customer Due Diligence should be treated as a minimum level of care, not an acceptable level. As noted at the start of the consultation, if the industry does not wish this level of scrutiny, they should be able to adopt a more conventional consumer protection approach of reimbursing victims and then assigning costs within the industry.

These standards should also rapidly adapt to changing criminal behaviours, including by identifying characteristics of fraud. For example, a common approach today seems to be to breach a customer's online banking and change the name of the account to be "FROZEN" and thus persuade the customer than they indeed should move money out of their account. Criminals use similar techniques and infrastructure for multiple frauds. It would be reasonable to expect firms to identify such characteristics of impending fraud and take action to protect the customer.

The standards are also too narrow and focus just on warnings – generic warnings as part of GF(1), more specific warning as part of SF1(2), and warnings relating to confirmation of payee in SF1(3). It is well established that customers suffer from "warning fatigue"[3] and just adding more warnings will at best do no good and at

[2] Progress and research in cybersecurity Supporting a resilient and trustworthy system for the UK, Royal Society, July 2016. https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf

[3] Security Fatigue, Stanton et al. IT Professional 18(5), October 2018. https://www.computer.org/csdl/mags/it/2016/05/mit2016050026-abs.html

worst harm security. Firms should be required to show that customers know how to perform transactions securely, and that these measures don't require more time or mental effort than would be reasonable for someone carrying out normal daily activities.

This guidance should include information on alternative ways to make payments. As in-branch payments and cheques are at lower risk to push-payment frauds, these measures should not be discouraged by banks. Credit and debit cards have different liability for fraud. Trade-offs in terms of revocability, liability and checks performed should be provided to customers.

An assessment as to whether a customer can be reasonably expected to know how to perform actions securely should not only take into account actions by the firm, but also the actions of other firms and industry bodies which the firm could be reasonably expected to know of, following the same principle as the Consumer Rights Act. This is because an individual's behaviour will be guided by the combination of the advice they receive. If a customer could reasonably be confused by advice that is contradictory, excessive or which requires excessive effort then they should not be held liable for fraud.

For example, one of my banks informed me by letter that they would never contact me and ask me to transfer money. Another of my banks called me and asked me to transfer funds from my current account to a savings account which the staff member would open for me and gave the reason that a savings account was a safer place to keep money. I contacted the bank branch and confirmed that this was a genuine call from the bank, and they were trying to promote savings accounts to their customers. Such behaviour could easily lead a customer to become confused about what industry advice to follow.

Currently the scope of the code is restricted to domestic payments and only to the firm which sends and first receives the funds. This may be which the current banking system allows to be done but doesn't meet the objective creating incentives to improve the banking system to allow more to be done. All payments which a customer can reasonably be expected to perform should be covered, and potential liability for fraud should include all firms which process a payment until it leaves the banking system (such as by being withdrawn by cash).

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.

If the Firm has not met their level of care the customer should still be reimbursed because otherwise there not be the incentive required by OP1(1) for Firms to meet their standards. Firms have full visibility over the payment process so can with reasonable confidence evaluate whether a customer has or has not met the level of

care specified in R2(1) – for example through showing a warning or flagging a negative Confirmation of Payee result. In this case a Firm would be free to make a cost-based decision to not apply further fraud prevention mechanisms, such as manual review of the transaction or contacting the customer, which may incur expense or inconvenience to the Firm.

It could be claimed that the same argument applies to customers, but this is implausible. Even if a customer thinks they are likely to be reimbursed, the stress and inconvenience of disputing a transaction and being without funds for almost two months is a strong motivation for them to act with appropriate levels of care. Customers are also unlikely to know whether or not a bank is going to act with due care in carrying out a transaction. It's implausible to claim that a customer is going to act negligently on the off-chance that a bank might have failed to meet the requisite level of care.

For this reason, the requirement of R2(2) that Firms should "consider" whether they could have done more. This vague specification leaves Firms free to act in their own financial interest to deny refunds for frauds that a diligent firm would have prevented. Such a specification is likely to result in inconsistent outcomes, in contravention to CP(2), and offers insufficient to form a consideration for the Financial Ombudsman Service, in contravention to CP(8).

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

Customers are entitled to have a reasonable expectation that the payment system is safe. This expectation is reinforced through banks' marketing material. Due to cost-saving measures resulting in bank closures and the push for customers to use FPS, customers are increasingly being discouraged to use in-branch transactions and cheques – both less vulnerable to push payment scams than online-banking FPS transactions. The onus therefore should be on firms to take on the responsibility for making online banking safe.

For this reason, R2(1) should specify that in order to refuse a refund they must demonstrate that a customer acted with "gross negligence". This is the level of care specified in the Payment Services Directive and therefore facilitates the base of precedent resulting from court decisions and those of the Financial Ombudsman Service. This would also allow the code to take advantage of the result of UK Finance's efforts to define "gross negligence" with more clarity[4]. The current terms in R2(1) could then be indicated as considerations when assessing whether a customer

[4] UK Finance response to the APP scams steering group's draft voluntary code, 28 September 2018. https://www.ukfinance.org.uk/uk-finance-response-to-the-app-scams-steering-groups-draft-voluntary-code/

has acted with gross negligence, but ultimately this assessment must be made in the full context of the situation.

It is certainly inappropriate to elevate the importance of warnings and Confirmation of Payee as being sufficient in themselves as a reason to refuse to reimburse. Depending on the context of the situation, the fraud technique employed, and the way in which the warnings or confirmation of payee is shown, it is possible that a diligent customer could still be defrauded. In such circumstances the victim should be reimbursed.

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

Due to the large sums typical for push payment scams any delay in reimbursement is likely to cause substantial distress. An ambitious schedule for reimbursement is therefore justifiable, as would interim support to mitigate hardship. If a decision to reimburse has been made and communicated to the victim, this is should be the final decision and must not be subsequently revoked. In my experience of assisting victims of unauthorised transfers, a frequent scenario is the victim to initially be reimbursed but later the bank reverses the reimbursement and claims that the customer authorised the transaction. This puts victims at a disadvantage because this delay in the eventual denial of reimbursement means that the customer would not have the opportunity to make a request the retention of evidence such as CCTV which could support their case before it is deleted. If a decision is made to not reimburse a victim, the sending firm should automatically retain information relevant to the case which may be called for in resolving the dispute in the FOS or courts and instruct other participants in the payment to do the same.

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, customers should be reimbursed, regardless of the actions of the firms involved. If a fraud occurs in a payment system despite all parties acting properly then this shows that the payment system is flawed and should be improved. Not reimbursing the customer in such circumstances would violate OP1(1) by not incentivising the industry to reduce fraud in such circumstances.

Push payment fraud is only possible as a result of the irrevocable nature of such payments and is facilitated through the push towards online and mobile payments in preference to cheque or in-branch transactions. As a result of branch-closure programmes, some customers may not even have an effective option of in-branch

payments. Customers have little influence over such industry decisions, particularly due to the lack of competition in the UK banking industry.

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?

As noted in the beginning of my response, having the sending firm not be responsible for reimbursement is an unconventional approach to consumer protection and therefore introduces difficulties. One way that this exhibits itself is that by administrating the reimbursement the sender is responsible for making the case as to whether the receiving firm met its standards. Because it is proposed that the sending firm will not be liable for the reimbursement if it has met its own standard of care, the sending firm will not have an incentive to demonstrate that the receiving bank has failed to meet its standard of care. If it is easier to make a case that customer failed to meet the needed level of care, when compared to making the case that the receiving bank failed to meet its level of care, there is no incentive to protect the customer because both options are cost neutral from the perspective of the sending bank. For this reason, in cases where the customer is not reimbursed there should be some penalty for the sending bank, to provide incentive for it to either have prevented the fraud or make a case that the failure occurred elsewhere in the payment system.

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

Whether a customer complies with required standards should be assessed by criteria developed by an independent party and be specific to the banking platform(s) in question. Following the operating principle of transparency, this assessment report should be made available to customers and be sufficiently detailed for them to be able to appoint an expert to repeat the assessment. The assessment should be performed according to the best-practices for evaluating security techniques[5], to ensure that the results of experiments are a valid representation of customers actual behaviour and the actual experience the customer would have while performing a payment. The criteria for a sufficiently

[5] Towards robust experimental design for user studies in security and privacy, Krol et al. LASER 2016
https://www.usenix.org/system/files/conference/laser2016/laser2016-paper-krol.pdf

secure system should be that all customers, taking ordinary care and in a realistic context, should have a proper understanding of the consequences of their actions and be able to reliably detect and prevent frauds.

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

The high costs and "loser-pays" model of the UK court system creates a significant problem with access to justice in the UK. Push payment scams commonly exceed the limit for the small claims court and therefore a customer pursuing a case in the courts is at risks of being required to pay the legal costs of their bank, likely a five-figure sum that few could afford. For all but the richest customers, this situation effectively eliminates the option of escalation to the court system.

As found by the Civil Justice Council, the current situation particularly affects customers[6][1]:

"Existing procedure does not provide sufficient or effective access to justice for a wide range of citizens, particularly but not exclusively consumers, small businesses, employees wishing to bring collective or multi-party claims. … There is overwhelming evidence that meritorious claims, which could be brought are currently not being pursued." The Financial Services Bill 2009 incorporated provisions to allow collective proceedings regarding financial products, in order to spread the risk of legal costs over multiple members of a class. However, the Financial Services Act 2010, as passed, had this provision removed.

The Financial Ombudsman Service offers an alternative dispute resolution system but is still insufficient because few customers can afford the specialist legal and technical expertise needed to argue the complex points that would be raised when raising a dispute under this code. In particular, arguments about the effectiveness of fraud detection schemes cannot be made by examining only an individual case, but instead need a statistical argument based on data held by the firm.

For this reason, the dispute resolution scheme should allow collective actions as proposed by the Civil Justice Council. This would allow the costs of legal and technical expertise to be shared over multiple claimants which share some common characteristics or raise related matters over the interpretation of the code. The scheme should be designed to provide incentives for legal and technical experts to assist in such collective actions and oblige firms to disclose technical evidence to

[6] Civil Justice Council. Improving Access to Justice through Collective Actions. November 2008. https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/CJC/Publications/CJC+papers/CJC+Improving+Access+to+Justice+through+Collective+Actions.pdf

allow the effectiveness of their detection and prevention measures to be assessed.

Q23 How should the effectiveness of the code be measured?

The Code permits the Firms significant discretion on whether to refund a fraud victim, resulting from the subjective criteria in R2 and possibility of ex-gratia payments (OP2). This discretion may inadvertently result in discrimination, as has been found in the case of reimbursement for other financial disputes[7]. Following Core Principle 2 (consistency of outcomes), and the Operating Principle of transparency, statistics should be collected and published on a per-Firm basis which show the fraud levels and reimbursement rates both overall for the Firm and split out by characteristics protected by Equality Act, as well as by indicators of wealth and profitability for the Firm.

These statistics would also facilitate the PSR's competition directive, allowing customers to select a payee bank which is more likely to protect their money and thus also facilitate the Core Principle 1 of the Steering group by creating an incentive for banks to reduce the level of push payment fraud. It is not sufficient for these statistics to be provided to the trade bodies and withheld from customers, as proposed in GF(2), because the code assigns cost of security failures to customers in some circumstances, and the choice of a sending bank is one which the customer must make.

[7] Banks biased against black fraud victims, The Times, 12 January 2017. https://www.thetimes.co.uk/article/banks-biased-against-black-fraud-victims-237z7rxvm