Response to consultation on authorised push payment scams

Dr Steven Murdoch, University College London

Throughout the responses to the consultation, I will refer to three principles which are necessary for the managing incentives within a model for assigning liability for adverse events, such as push payment fraud. These principles are selected such that liability is assigned fairly, and that the party in a position to reduce the risk of future adverse events is incentivised to do so.

1) Avoiding conflict of interests through independence

When a process deals with assignment of liability between members of a group (internal assignment of liability), it is acceptable that the process is developed, maintained and monitored by that group or an organisation that the group appoints. However, when the process may assign liability to a party outside this group (external assignment of liability), then the development, maintenance and monitoring of the process must be handled by an independent party which has the responsibility to represent the interests of all parties to which liability may be assigned, and has the resources and expertise to effectively discharge this responsibility. Otherwise, it is likely that the organisation controlling the liability assignment processes will dump risk on parties less able to mitigate said risks, and hence reducing the incentive to prevent future adverse events.

2) Transparency and accountability

No liability-assignment process is perfect, nor can it be ensured it is followed perfectly. Therefore detailed records should be created of who made what actions while following the process, when, for what reason, and with which result. These records should be retained for an appropriate period and made available to any relevant party, in particular individuals or institutions who may have the liability assigned to them. This principle is necessary to allow effective monitoring, and to facilitate the resolution of disputes through external arbitration, or in the courts.

3) System-operator responsibility

The organisation which operates a system should accept responsibility when there is an adverse event that results from the use of that system. As stated in the Royal Society report on cybersecurity[1]:

"To improve security, responsibilities should be assigned to parties that could effectively discharge them, and could afford to do so. Consumers typically have the least capacity to mitigate risks, while service providers can improve security through system design and implementation, and by taking careful account of real-world use of

1 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

their products. In most cases this means liability regimes should protect consumers, and prevent system operators from shifting liability to individuals where it is not reasonable to do so."

Question 1: In your view, will the best practice standards developed by UK Finance be effective in improving the way PSPs respond to reported APP scams? Please provide reasons.

The best practice standards will likely improve the current handling of push payment fraud complaints, and to the extent that these standards deal with internal assignment of liability between the organisation who UK Finance represent (the PSPs), I think it is appropriate that UK Finance develop, maintain and monitor these processes, with regulatory oversight to manage systemic risk and social costs resulting from fraud.

However, when standards affect liability outside the group of PSPs and so potentially assigning liability to PSP customers (as proposed in the contingent liability model) UK Finance should not be responsible for the development, maintenance and monitoring of the standards. The role of UK Finance is to act representative of the finance, banking, markets and payments-related services, as publicly stated and demonstrated by the organisations represented on its board (18 are from industry and only 1 represents the interests of customers). Therefore, while UK Finance should contribute the views of their member organisations, following the principle of avoiding conflicts of interests, the organisation responsible for the standards which PSPs must follow should be independent and have the responsibility to represent both customers and PSPs, and have the ability the ability to effectively discharge this responsibility.

Question 2: Should a contingent reimbursement model be introduced? Please provide reasons.

A contingent reimbursement model does not follow the principle of system-operator responsibility, and therefore creates an opportunity for PSPs to unfairly dump liability onto customers and so reduce the incentive of PSPs to prevent fraud. The contingent reimbursement model therefore creates an necessity for strict oversight to mitigate this risk (such as creating an independent organisation to manage standards for PSPs, discussed in the answer to Q1). Were liability assigned to the system-operators, a more light-touch regulatory approach could be adopted while still ensuring that customers are protected and system-operators are incentivised to reduce fraud.

However, should a contingent reimbursement model be adopted (as the consultation indicates to be the preference of the PSR), there are ways by which the risk of liability dumping can be partially mitigated (at the cost of requiring much greater external scrutiny), as will be discussed in answers to other questions.

Question 3: Do you agree with our high-level principles for a contingent reimbursement model? Please provide reasons.

As mentioned in Q2, there are significant risks to customers of a contingent reimbursement model. However on the assumption that this is the model to be adopted I discuss appropriate criteria for setting PSP standards and customers requisite level of care in the answers to Q5 and Q9 respectively.

Question 4: In your view, what are the relative advantages and disadvantages of each alternative outcome for a 'no blame' situation (the victim is reimbursed by PSPs, or the victim bears the loss)? Please provide reasons.

Following the principle of system-provider responsibility, I consider that in the "no-blame" situation, the customer should not be held liable. In the no-blame scenario, fraud has occurred despite all parties acting properly, and therefore implies that the system is insecure. The system-operator should accept responsibility for the failure, and if the level of "no-blame" fraud exceeds levels the operator considers acceptable, the system should be improved.

If the customer were held liable in the "no-blame" situation then the system-operator would have no incentive to address vulnerabilities in the system which could allow fraud to occur in this scenario.

Furthermore, when PSPs are held liable, they have the ability to accurately estimate the risk to their business and obtain insurance or opt-to self insure, spreading risk over their customers. Customers, in contrast, have little awareness of risk and do not have effective access to insurance, and so while only a small proportion of customers are affected by push payment fraud, the impact on their lives can be devastating.

Question 5: Do you agree that the measures being developed by industry (specifically UK Finance and the Forum) should be included as the required standards of the contingent reimbursement model that PSPs should meet? Please explain your reasons.

For the same reasons noted in the answer to Q1, required standards that affect liability assignment should be developed, maintained and monitored by an independent party set up, and able to, represent the interests of both customers and the payments industry. As such, organisations such as UK Finance and the Payments Strategy Forum should be able to contribute to these standards but customers must be strongly represented in order for the continent reimbursement model to achieve its goals of protecting consumer rights and providing incentive for system improvements.

The measures developed by industry so far go some way towards preventing push payment fraud, but do not go far enough. The results of research on payments fraud at University College London and elsewhere show further opportunities for which PSPs should improve before being able to assign residual risks to customers:

1) Clear description of fraud liability and revocability of different payment options

Customers have several payment options available to them, but for PSPs encourage ones which are cheaper to carry out (e.g. Faster Payment Service – FPS) over more

expensive ones (e.g. cheques), despite the likelihood of fraud and liability that results being significantly different. For example, as the consultation document notes, payee name is not verified for FPS, and thus is more vulnerable to maliciously misdirected payment fraud. In contrast, it is the responsibility of the beneficiary's bank[2] to verify the name on crossed cheques. To give customers the ability to effectively control their risk, payment systems with less effective fraud prevention should not be promoted over payment systems which from the customers' perspective may be safer, and customers should be clearly informed of the liability-assignment arrangements for each payment method they have available.

Similarly, push payment fraud is made easier as a result of FPS transactions being immediately irrevocable[3], even though it is not clear that this property is always desired by customers. In contrast, cheque payments may be revoked up to 6 working days after deposit. The payment industry could make available an alternative to FPS where funds would appear in payers account immediately, but like cheques, remain revocable for some period in cases of push payment fraud. In many cases where FPS is used, the payer and payee have an ongoing business relationship and so the risk of the payee fraudulently revoking the transaction is limited, but it would make push payment fraud much more difficult to conduct. An irrevocable payment system like CHAPS could be made available, provided payers are made aware of the risk.

2) Improved transaction authorisation, that leads to appropriate mental models

The payments which are the subject of this consultation are termed "authorised" because the payer has provided security credentials which his or her bank consider sufficient. However this is not actual authorisation by the ordinary definition of the word (where it refers to the state of mind of the payer i.e. that they have given their consent), because in the case of a maliciously misdirected payment the payer did not actually consent that the payee receive these funds. The customer might have authorised a payment to someone they know, or authorised a transfer to the payers own account, but because he or she did not have a sufficiently accurate mental model of how the PSP's system works, the security credential the payer's bank received are sufficient to cause a fraudulent payment.

Initial results from our ongoing research on this topic have shown that small changes in the transaction authorisation process can significantly affect the mental model of payers understanding of the payment process, and consequently what steps the customer will take to avoid fraud. In some cases we have examined, the customers act in such a way that they would be able to detect fraud. With other PSP's system, customers naturally are led to have an incorrect understanding of the process, and hence vulnerable to fraud even if they are taking what they consider to be requisite care. PSPs should only be able to disclaim liability if they can empirically demonstrate that their transaction authorisation system will lead customers to act in a way that would allow them to readily prevent fraudulent transactions.

---

2 Bills of Exchange Act, 1882

3 Ross Anderson, Closing the Phishing Hole – Fraud, Risk and Nonbanks. At Nonbanks in the Payment System, May 2007. https://www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf

3) Assessing compliance to required standards

Whether a PSP complies with required standards should be assessed by an independent party, and following the 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[4], to ensure that the results of experiments are a valid representation of customers actual behaviour. The criteria for a sufficiently 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.

Question 6: If a contingent reimbursement model is introduced, which organisation should design and implement it? Please provide reasons.

Existing organisations and processes within the payments industry that I am aware of are responsible for allocating liability between member organisations, whereas a contingent reimbursement model is significantly different in that the outcome of the process may be that the customer is held liable. For this reason I expect it will be necessary that a new organisation, independent from the payment industry, will need to be created to manage the process.

Question 7: In your view, are there any barriers to the adoption of a contingent reimbursement model which we have not considered? Please provide reasons.

The Payment Services Regulations allows the Financial Ombudsman Service (FOS) to act as an alternative dispute resolution service, presumably including over the use of a contingent reimbursement model. However, in cases where the FOS is not able to resolve a dispute to all parties' satisfaction, the dispute will need to be referred to the court system. The court system also serves a critical role as a check-and-balance to the fairly opaque and unaccountable ombudsman process. Furthermore, courts have powers which are unavailable to the FOS, such as to make and enforce orders for the disclosure of evidence, set precedent, and appoint independent experts.

However, the high costs and "loser-pays" model of the UK courts creates a significant problem of access to justice. Push payment scams commonly exceed the limit for the small claims court and therefore a customer pursuing a case in the courts is at risk 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.

The Civi Justice Council found that this situation particularly affects customers[5]

---

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

5 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

"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.

In contrast, many other countries either have each litigant pay their legal costs in normal circumstances, or at least cap the customer's cost to a level they can afford. Therefore, while other countries may have a default assignment of liability for push payment scams to the payer, similar to the UK, they have better access to justice and therefore have a more effective means to challenge this decision. While the PSR cannot change this situation by itself, any contingent reimbursement model will effectively be the final decision for the vast majority of customers, and so should replicate the features of the court system that are needed to fairly resolve cases.

Question 8: Please explain, if relevant, how your organisation currently decides whether to reimburse a victim of an APP scam. Does this include an assessment of vulnerability?

Not applicable.

Question 9: Are there any factors that should be considered when defining the requisite level of care victims should meet?

As discussed in the answer to Q4, the system-operator is in the best position to influence customer behaviour in order to reduce risk of fraud. Therefore the minimum level of requisite care should anything other than gross negligence, as with the Payment Services Directive 1 and 2. When assessing whether a customer has been grossly negligent, the actions of a customer should be examined to see if they fall far short of what a reasonable person would do in a comparable situation, taking into account pressures that customers are subject to, and what practices have been encouraged, or at least tolerated by, the PSP involved in the fraud and other PSPs which the customer deals with. Our research has found that security instructions described in terms and conditions (T&C) of PSPs are inconsistent, confusing[6] and far exceed what customers do in practice and what they can achieve with realistic effort[7]. Therefore gross negligence should not be defined in terms of non-compliance to T&C.

---

6 Becker et al. International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Term. Workshop on the Economics of Information Security (WEIS), June 2016. http://sec.cs.ucl.ac.uk/users/smurdoch/papers/weis16fraudreimbursement.pdf

7 Murdoch et al. Are Payment Card Contracts Unfair? Financial Cryptography 2016. http://sec.cs.ucl.ac.uk/users/smurdoch/papers/fc16cardcontracts.pdf

Where compliance with PSP provided customer education forms a part of the assessment of requisite level of care, PSPs should provide empirical evidence that the information provided to their customers regarding secure behaviour, as well as the means of communicating this information, are easy to understand, easy to remember, consistent across all means of communication and consistent with the design of other technologies associated with this bank and that of other banks common in the region. Following the principle of transparency, this evidence should be provided to customers so that they can examine and challenge whether the PSP have discharged their duty adequately.

Question 10: Do you think it is necessary for a significant majority of, if not all, PSPs that provide push payment services to consumers to adopt the contingent reimbursement model for it to be effective? If yes, please explain if you think the model would need to be mandatory for PSPs

Competition within the retail banking industry has not been particularly effective at improving quality of service, as shown by the low rate at which customers move banks. For example, the Competition and Markets Authority found[8] that over half of customers had been with their current account provider for more than ten years, concluding that "we have therefore found that competition in [personal current account] markets is not working well."

The UK banks have also generally made a policy decision to not compete on security and so here especially, competitive pressures have not been effective at reducing risk to customers. While the retail banking market investigation of the Competition and Markets Authority have recently enacted some measures to improve competition (e.g. Open Banking), these have not yet had a significant effect. For this reason I would consider it appropriate that any reimbursement model be mandatory.

Question 11: What are your views on the scope we have outlined for the model? Please describe any other factors you think we should consider.

As a result of initiatives like the IBAN and SEPA, the distinction between domestic and international transfers are increasingly indistinguishable to customers, and therefore it seems inappropriate to assign risk of push payment fraud to customers in the case of overseas accounts. If the system design for international payments is not secure enough to effectively recover funds, then system operators should be given the incentive to resolve this deficiency.

Question 12: In your view, how should the dispute resolution mechanism work and which organisation should oversee this? Please provide reasons.

I am not aware of an existing organisation who could oversee this dispute resolution

---

8 Competition and Markets Authority. Retail banking market investigation (final report). August 2016. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

mechanism and because of the risk of liability dumping, procedures must be set up to ensure transparency and independence of the organisation responsible for making decisions. As such, the body responsible should be independent of the banking industry and be provided with sufficient independent technical and legal resources to fairly resolve disputes.

Question 13: Do you agree with our view that a contingent reimbursement model, if introduced, should be in place by the end of September 2018? Please explain.

As a result of the work by the PSR, we know the substantial financial and human cost that push payment fraud imposes on individuals and society. Therefore mitigations, such as the contingent reimbursement model should be introduced as a matter of urgency.

Question 14: Should a phased or transition approach be used to implement a contingent reimbursement model? Please explain.

As noted in the answer to Q13, the sooner mitigations are introduced, the better it will be for customers and the greater will the incentive be on PSPs to reduce the risk of fraud. The precise timing of the introduction of mitigation should be considered by an independent body taking into account the views of the payments industry and representatives of customers.