Response to Financial Conduct Agency consultation paper CP18/16: Authorised push payment fraud – extending the jurisdiction of the Financial Ombudsman Service

Dr Steven J. Murdoch, University College London
September 2018

Q1: Do you agree with the Glossary definition for APP fraud? Please explain why.

The two definitions provided (impersonation and purchase) do appear to be within the consensus definition of Authorised Push Payments (APP). However, the definition excludes a third case which has been discussed both in the context of inclusion within the Contingent Reimbursement Model (CRM), and by Payment Service Providers (PSP) who have refused to refund alleged victims of fraud.

Specifically, this excluded case – which I refer to as authorisation code disclosure – is where the customer is tricked into disclosing an authentication code which is dynamically bound to a fraudulent transaction, without realising that this authentication code would allow such a transaction to be performed. An example of this case is where the authentication code is generated through an EMV Chip Authentication Program (CAP) device and the sending customer's debit card and PIN. My research [1] has shown that a criminal could instruct a customer to interact with the CAP device in order to generate an authentication code which the sending PSP would accept, without even a diligent customer being aware that this code would allow a transaction to be performed.

From the perspective of the sending PSP, authorisation code disclosure may be indistinguishable from the impersonation scenario because the PSP will receive the same security credentials and authorisation codes as they would if the customer intended to transfer money to the destination account in question. Through the use of off-the-shelf Man-in-the-Browser malware, the criminal would also be able make the fraudulent transaction appear to be initiated from the customer's normal browser and IP address.

There is a strong case for including authorisation code disclosure within the cases where the victim of fraud could raise a dispute with the receiving PSP. Whether this is done through expanding the definition of APP, or through expanding the circumstances in which the new dispute procedure could be invoked, is of less importance. I will expand on this point in my answer to Q2.

[1] Optimised to fail: Card readers for online banking, Financial Cryptography and Data Security (2009) https://murdoch.is/papers/fc09optimised.pdf

Q2: Do you agree with our proposal to apply our complaints handling rules to complaints by payers against receiving PSPs about a failure to prevent alleged APP fraud, and bring these complaints into the Financial Ombudsman Service's CJ and VJ? Please explain why.

I think the proposed changes to the Financial Ombudsman Service (FOS) jurisdiction will be an improvement to the current situation, but they have two important gaps – the exclusion of important scenarios such as authorisation code disclosure and there being insufficient measures to allow victims to effectively raise a dispute with the receiving PSP.

I discussed the case of authorisation code disclosure in Q1. In cases where the customer is refunded by the sending PSP, there will not be any dispute raised with the FOS and so is not relevant for the purposes of this consultation. I will therefore only focus on cases where the sending PSP refuses to refund an alleged victim.

In my experience, PSPs who refuse to refund a disputed transaction alleged to have been performed through such a technique do so either by arguing the a customer has been grossly negligent in disclosing the authorisation code (and therefore under the Payment Services Regulations (PSR) 2017 77(3) is liable) and/or the act of generating the code was equivalent to authorising the transaction (and therefore is not considered to be unauthorised for the purposes of PSR 2017 77 at all). It is not necessary for the PSP to demonstrate which of these two alternatives occurred in order to refuse a refund, only that one of these two alternatives is the likely explanation for the transaction. As I noted in my answer to Q1 the two cases are possibly indistinguishable to the PSP, and rarely are the actual facts of a case established with any degree of confidence.

Regardless of whether the customer is considered to have authorised the transaction or was negligent, it is in the interests of the FCA's operational objectives of consumer protection and integrity to create incentives for the receiving PSP take reasonable steps to prevent or reverse such fraudulent transactions. An effective way to create financial incentives is to allow the inclusion of authorisation code disclosure within the shared-blame scenario of the CRM if both the customer and receiving PSP have acted without the requisite level of care. Resolution of such cases is only possible if the FOS has jurisdiction to handle them.

For this reason, I think there is a strong case for the jurisdiction of the FOS to handle disputes between a customer and receiving PSP to be expanded to include the authorisation disclosure case. There may be other such scenarios which arise in the future, so my preference would be to allow customers to bring complaints to the FOS regarding the receiving PSP's handling of a fraudulent transaction regardless of how the alleged fraud was performed.

The second way in which I consider the proposed changes to be insufficient is that procedures designed for raising a dispute with the sending PSP are not enough when the dispute is with the receiving PSP. This is because an alleged victim has no business relationship with the receiving PSP (whereas they have contractual relationship with the sending PSP) and it is the criminal, not the customer who selects the receiving PSP. These factors mean that the alleged victim has no means to collect information that they need to demonstrate that the receiving PSP has acted without the requisite level of care, and market forces will not incentivise PSPs to improve their handling of fraudulent transactions.

I would therefore recommend that the dispute procedures include requiring that receiving PSPs disclose to a customer raising a dispute with them, any documents regarding their procedures for preventing and reversing fraudulent transactions received, any audit reports (whether internal or external) regarding the effectiveness of these procedures and how they compare to other PSPs, as well as records showing how the transaction(s) that are the subject of dispute were handled. These documents would put customers in a better position of showing whether the procedures were adequate, whether they met accepted industry standards, and whether the procedures were followed correctly. Due to recognised problems about access to justice in the UK [2], the FOS will likely be the final level of dispute resolution available to most customers and so the disclosure procedures of the civil court system cannot be assumed to be available to serve this purpose.

I recognise that PSPs may be uncomfortable with disclosing this information, but I would respond that this is a necessary consequence of the CRM adopted by the industry. The need for the CRM in the first place is the result of deliberate industry cost-saving measures of moving transactions away from the relative safety of bank branches to the far less safe online environment, and therefore allowing branches to be closed or refocussed on more lucrative financial products [3]. If PSPs wish to avoid having to disclose information about how the receiving PSP meet the requisite level of care for handling fraudulent transactions the sending PSP is free to reimburse the victims of fraud and then be reimbursed themselves by the receiving PSP through an internal industry dispute resolution process [4]. For PSPs to both want to profit from the reduction of costs resulting from online transactions, and simultaneously avoid scrutiny over how fraudulent online transactions are prevented, would not be in the interests of consumer protection nor the integrity of the UK financial system.

[2] 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
[3] "The branch is dead"? Where will customers bank tomorrow? The American Banker, July 2013 https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-the-branch-is-dead-customers-bank-tomorrow-062017.pdf
[4] Response to consultation on authorised push payment scams, Steven Murdoch https://www.benthamsgaze.org/wp-content/uploads/2018/06/pushpayment_murdoch.pdf

Q3: Do you support a wider voluntary scheme, run by the Financial Ombudsman Service, to cover complaints which are not covered by our proposals? If yes, what do you suggest such a scheme should cover?

I would support the expansion of the FOS jurisdiction but in the interests of transparency and fair competition consider this better achieved through a mandatory rather than voluntary scheme.

Q4: Do you agree with our proposal to give effect to the requirement to bring these complaints (about a payee's PSP's cooperation with the payer's PSP to recover funds involved in a payment transaction where incorrect details have been provided) into the Financial Ombudsman Service's CJ and VJ? Please explain why.

As noted in my answer to Q2, I would support the proposal with the caveats that improvements are needed both in terms of expanding the scope of complaints and enhancing the transparency of procedures to allow a customer to effectively raise a dispute through the FOS.

Q5: Do you agree with the costs, benefits and transfers we have identified? If not, please explain why.

With the caveats listed in my answer to Q2 I think the analysis is broadly appropriate.