Response to Home Affairs Committee inquiry into Fraud

https://committees.parliament.uk/committee/83/home-affairs-committee/news/197427/home-affairs-committee-launches-inquiry-into-fraud/

Submitted by:

- Richard Emery, 4Keys International.
- In my capacity as an Ambassador for the Transparency Task Force.

Thank you, Home Affairs Committee

I am very concerned about the levels of fraud in the UK; and I believe the evidence shows there is urgent need for reform.

I (along with my colleagues at the Transparency Task Force) am therefore very grateful to the Home Affairs Committee for the opportunity to feed in to this important inquiry on fraud. We stand by ready to support your reform agenda in any way that we can. In particular, we would like to suggest a meeting to discuss this input once you have had time to review it. I am happy for this submission to be published.

Personal Background

My early career focussed on the business use of IT in retail, logistics and payments. I have served as an expert witness in civil and criminal matters for 25 years, primarily in cases regarding theft and fraud. For the last 8 years I have been assisting people who have been the victims of bank fraud to challenge their banks and take complaints to the Financial Ombudsman Service. I have given oral evidence to the Treasury Committee and interacted with both the FCA and PSR in respect of recent consultations regarding developments in fraud prevention and reimbursement. I serve in the Secretariat of the APPG on Personal Banking and Fairer Financial Services, and as mentioned I am an Ambassador of the Transparency Task Force, a Certified Social Enterprise with a mission to “promote ongoing reform of the financial sector so it serves society better”.

1. Introduction

2. This submission focusses on three of the points raised in the Call for Evidence:

- The role of Internet Service Providers (ISPs) and Telephone Service Providers (TSPs),
- The effectiveness of the current system for reporting fraud and initiating Police investigations.
- Whether the Fraud Strategy (FS) is resulting in the banks doing enough to prevent fraud.

3. It is based on my personal experience of assisting victims over the last 8 years. The names have been changed to protect their identities.

4. The Role of ISPs and TSPs

5. The case study on page 19 of the Fraud Strategy, about the success of the Metropolitan Police to take down the iSpoof website, is clearly an important step forward. The Ofcom consultation on the introduction of Calling Line Identification (CLI) authentication technology (paragraph 97 of the FS) is another helpful development and should be pursued.

6. I suggest that the Committee should consider supporting three further developments:

a) A consumer education programme that clearly explains what CLI is and, more importantly, that it cannot be trusted.

b) All TSPs should be required to prevent calls that originate from overseas presenting what appears to be a UK CLI, thus reducing the ability of overseas fraudsters to pretend they are calling from within the UK.

c) The rapid expansion in the use of "Do [or Does] Not Originate" (DNO) across all financial services and related businesses, regulators etc. The DNO service allows organisations to register telephone numbers which they never use to make outbound calls, and which should not, therefore, ever appear on a consumer's phone as a CLI. This is particularly important for numbers which consumers can 'verify' as being 'genuine'. One example of this is when a fraudster contacts a potential victim, they may invite them to check that the number displayed on their phone is the same as the phone number on the back of their debit or credit card. This is an important part of the process of socially engineering the victim into believing that the call is genuine. Amy lost £525,000 because she believed the caller was from her bank.

7. The Effectiveness of Reporting Fraud and Providing Information to the Police.

8. It is encouraging to read that [In]Action Fraud is going to be replaced by a new 'Fraud Reporting Service', but it is important to recognise that the new service will need to be a vast improvement on the current service, and not just a change of name.

9. A vital part of the work of the new service, which Action Fraud have been very poor at doing, will be the identification of frauds that have a common thread. In August 2022 a Police force started an investigation into an alleged investment fraud involving £10m lost by c.180 victims. I made it clear to the victims who I was assisting that it was important for them to report the fraud to Action Fraud so that their details would be passed onto the Police. Despite their reports clearly naming the company behind the alleged fraud several of them received 'standard' responses saying that their report could not be linked to any current investigation. This was simply not good enough.

Case Study - Bank Ignores Fraud Warning

10. Failure to respond appropriately to fraud warnings goes beyond Action Fraud.

11. Shortly after making his third payment of £25,000 into an investment fund John tried to contact the investment company, only to discover that he was the victim of fraud. He contacted his bank, but they declined to reimburse him.

12. He was unwilling to just walk away from the loss and pursued his own enquiries. In the course of his investigation he obtained documentary evidence that several months before he became a victim of the fraud his bank had been contacted by the National Fraud Investigation Bureau (NFIB) because they had linked the account to a possible fraud, but the bank had done nothing about it. I was able to review the account history for the previous 12 months and it was clear to me that the account activity was at least suspicious, and that if the bank had investigated the NFIB report the account would have been closed down long before John became a victim.

The Police Response - Skills and Resources

13. I am encouraged to read the Home Secretary's commitment to the development of new National Fraud Squad (NFS) and Regional Organised Crime Units (ROCUs) with over 400 new specialist investigators, and making tackling fraud a priority for police forces in England and Wales.

14. But:

* The 400 new investigators are not enough. It represents just 0.25% of the total UK Police, increasing the percentage of Police resources from 1% to 1.25% to tackle fraud that now accounts for over 40% of all crime.
* There is no commitment to ensure that officers who are allocated to this vital work will not be quickly re-allocated to other areas.
* There is no clear skills development plan in this increasingly complex and challenging area of investigation.

15. The Government's Fraud Strategy

The True Level of APPFraud.

16. Paragraph 12 of the Fraud Strategy notes that "Industry reporting suggests average personal losses for authorised frauds (these are frauds where the victim has approved a payment) could be almost £3,000". This is according to figures published by UK Finance.

17. Whilst accepting that the figure of £3,000 is mathematically and statistically correct, it hides the impact of Authorised Push Payment (APP) Fraud in the more serious cases.

18. Figures published by UK Finance in their Fraud Report 2023 reveal that just 3.3% of APPFraud cases considered under the CRM Code represent 57% of the total value of losses, with an average value of over £33,000 each.

19. Although I am only a single independent fraud consultant, and not part of a larger group or company, I have successfully assisted 21 people who had lost a total of over £5m, i.e. with average losses of nearly £250,000 each.

20. The banks, and the government, should be focussed on preventing cases like this.

21. So, what should the government and banks be doing to prevent APPFraud?

Really Important Matters Are Missing

22. I am not going to disguise my frustration at some of the statements made in the Fraud Strategy. It appears to me that the authors have not fully grasped some really important matters that need to be addressed.

23. Paragraph 32, in the section of the FS titled “The Harm Fraud Causes”, says that: “A new approach is needed to keep the public safe and reduce the national security threat.” but nowhere does it specifically state that the banks must do more to prevent fraud.

24. Any “new approach” must include clear, unambiguous, and enforceable actions that all Payment Service Providers, and most especially retail banks, must take to reduce the level of APPFraud.

25. Paragraph 75 correctly identifies that: “Companies [including the banks] are in a unique position to protect their customers from fraud.” and then mentions The Banking Protocol. The Banking Protocol has been successful at preventing fraud where the victim is trying to withdraw a large amount of cash, but less-so when the payment is being made online.

26. Paragraph 88 refers to: “UK Finance, [agreeing] a charter focused on preventing authorised fraud.” but they have also openly opposed a specific proposal that was put forward by the Treasury Committee in its report Economic Crime: Consumer View in November 2019 and which was endorsed by the House of Lords report Breaking the Chain in November 2022. I will expand on this point in my specific proposals below.

27. Paragraph 100 explains the benefit of Confirmation of Payee and reports that “The Payment Systems Regulator (PSR) has issued several directions to extend the reach of Confirmation of Payee (CoP) across industry to over 400 firms.” but this figure will not be reached for another year. The introduction of CoP has been, and continues to be, an inadequate response. When first introduced in 2020 it was limited to just handful of major banks; which I have described as “shutting the stable door without building the back of the barn”. Fraudsters could easily move their accounts to those banks that hadn’t been mandated to implement CoP. By way of comparison, when faced with the same fraud challenge, the Netherlands developed the IBAN-Name Check service called SurePay in 2016. This covers 99% of all of payments in the Netherlands and is used outside of banking to undertake name verification in other financial services.

28. Paragraph 102 recognises that: “that in a small number of cases it may be beneficial for payments to be held beyond the usual timescales established in legislation in order to better protect customers.” and then suggests the need for a change in legislation, ignoring Regulation 86 of the Payment Services Regulations 2017 (PSR2017) that already allows for payments to be held until the following business day. I will comment further on this point below.

29. Paragraph 103 appears to be a reference to the Consumer Duty that was introduced at the end of July 2023. It must be noted that the non-Handbook guidance to the Consumer Duty that was issued in July 2022 stated that "Firms must avoid causing foreseeable harm to customers." and included a specific reference in paragraph 5.23 to an example of "foreseeable harm " as "consumers becoming victims to scams relating to their financial products, for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers". This was an important requirement, but was not included in the Cross-Cutting Obligation in FCA Handbook at PRIN 2A.2.10. This removed some of the obligations on the banks to develop systems and process to prevent APPFraud.

30. Paragraph 130 focusses on reimbursement, which is a really important development, but continues to talk about: "providing greater incentives to PSPs and other industries to prevent these frauds in the first place", rather than imposing clear and specific obligations to prevent the frauds happening in the first place. Whilst welcoming the plans to introduce mandatory reimbursement we must recognise that this only applies in cases of APPFraud and a number of banks have been seeking to avoid paying out under the CRM code by asserting that cases were not fraud.

31. Paragraph 150 says that: "This strategy will be delivered in close partnership with three stakeholder groups". I note that group 3 is simply listed as "Partners across industry and the private sector" but does not make specific reference to the banks who must be major participants in preventing APPFraud.

32. Specific Proposals

33. Having been critical of many aspects of the Fraud Strategy I will now set out my specific proposals for preventing, or at very least substantially reducing, APPFraud.

24-Hour Payment Delay - Mandatory

34. It is widely recognised that fraudsters endeavour to socially manipulate their victims into authorising payments in a rush. They do not want the victims to speak with anyone else, or to have time to quietly reflect on the reasons for making the payment.

35. This proposal is that banks would not release payments of over £500 to a new payee (i.e. someone to whom the payer has never made a payment before) until a clear 24-hours after the payer created the new payee details in their account.

36. Certain types of APPFraud are particularly susceptible to time pressurisation, such as 'account transfer' fraud where the victim is persuaded (by someone who they believe to be their bank) that their account is under attack and that they must move their money to a new safe account immediately. In a similar way, fraudsters intercept emails from solicitors who are processing house purchases and give new account details on the same day that the purchaser needs to pay the deposit, meaning that the payment is rushed.

37. The banks have argued that:

    * this will be very inconvenient for their customers

    * such a delay is not permitted under PSR2017.

38. In 5 years of arguing for this policy I have identified just one case where a payer making a payment of more than £500 did not have the correct payee details at least 24 hours before the payee needed to receive the payment. Such rare situations could be easily overcome through a system of secure telephone authorisation.

39. The argument that a delay is not permitted under PSR2017 is the result of widespread misunderstanding of Regulations 86 and 89(3), and ignorance of paragraphs 8.273 and 8.293 of the FCA Approach to PSR2017.

40. In addition to giving the payer time to reconsider their actions, a mandated delay would give the sending bank a clear opportunity to review the payment, contacting the customer if needed.

41. This proposal was supported by both the Treasury Committee in their report "Economic Crime: Consumer View and by the House of Lords report "Fighting Fraud: Breaking the Chain".

24-Hour Delay - Optional

42. This proposal would allow customers to give a single instruction to their bank to never release any payments of over £500 (or some other value chosen by the customer) for a clear 24-hours after they had authorised the payment, even if they had made payments to that payee before.

43. It would be an 'opt-in' system.

44. The rationale behind this proposal is that with certain types of fraud, such as romance fraud or crypto investment fraud, the fraudster starts with a low value and then

manipulates the victim to make ever higher payments, knowing that these are unlikely to be red-flagged by the bank's systems.

45. The optional delay would allow time for the payer to reconsider their actions, and also creates time for the next proposal to happen.

Second party notification

46. I have assisted victims of APPFraud where the fraudster was relying on nobody else knowing what was going on. For example, an on-going high-value fraud was only stopped when the victim happened to mention to her son, during an occasional phone conversation, that she was assisting the FCA to investigate fraud at her bank.

47. This proposal is that whenever the bank sends a text message or email to a customer (who has signed-up for the service) that message is also sent to a 'second party'. The second party would typically be a son/daughter, or a parent, or a Carer. The message would notify the second party that something was happening, giving then the opportunity to contact the account holder (i.e. their parent, child or person they a caring for) to just check that all was OK. The second party would not have any authority to contact the bank or act on the person's behalf. It is quite simply, so that they would know and could intervene if they need to do so. Simple, practical and effective.

Bank ID

48. I ask a simple question: "When my bank phones me they take me through a security protocol. What does this protocol do? And what does it not do?"

49. It does prove to the bank that I am me.

50. It does not prove to me that they are my bank!

51. Successfully impersonating a bank is the first step to gaining access to the victim's accounts and persuading them to make payments that end up in the hands of the fraudster.

52. Why have the banks not addressed this obvious gap in their security protocol? They appear to be more concerned about protecting themselves than protecting their customers.

Suggested next steps

As mentioned earlier, I would like to suggest a meeting to discuss this input.

Richard Emery
4Keys International
30 Farley Copse
BRACKNELL
RG42 1PF

Richard@4keys.co.uk

01344 484235
0777165 6638

19th October 2023