Richard Emery – Written evidence (FDF0040)

INTRODUCTION

My primary role as an Independent Bank Fraud Investigator is to assist individuals who have been victims of Authorised Push Payment Fraud (APPFraud) to challenge the banks and, if necessary, to take their complaints to the Financial Ombudsman Service. I also support groups of people where they are the victims of exactly the same fraud.

In addition to assisting victims of fraud I work with the APPG on Personal Banking and Fairer Financial Services, and with the Lending Standards Board, and I raise strategic matters across the banking industry.

I confirm that I am making this submission in a personal capacity.

SUMMARY

The general perception of the Fraud Act is that it has a narrow focus on convicting those who commit fraud, so I am pleased to see that this inquiry is taking a much wider view and encompasses both the prevention and investigation of fraud.

This submission will, therefore, consider the following statements:

A) The banks, and related technology companies, have failed, are failing, and will continue to fail, to prevent Authorised Push Payment Fraud (APPFraud) unless both the regulatory landscape and the enforcement of that landscape are substantially enhanced to reflect the exponential growth in APPFraud, which I estimate will exceed £1bn in 2022.

B). Why should fraudsters be concerned about being caught and convicted when 40% of all crime is economic but less than 2% of police budgets is spent fighting it, and there is a woeful lack of experienced officers and civilian staff dedicated to the task?

FRAUD LANDSCAPE

1) UK Finance have not yet published 'Fraud the Facts' for the whole of 2021, so the best official figures that we have are for Jan-June 2021. APPFraud amounted to £355.3m during these six months, representing a 71% increase on the same period in 2020. Included in these figures was the shocking rise of 131% in impersonation fraud.
2) By taking into account the overall growth in APPFraud, and the typical increase between the first and second halves of the year, I estimate that the full year figure for 2021 will be above £750m, rising to more than £1bn in 2022.

Q1. What fraud risks are UK individuals particularly vulnerable to today, and what are the reasons for this?

3) The top three fraud cases that I see are, in no particular order:
4) **Impersonation fraud** (often resulting in account transfer fraud

5) Fraudsters can easily impersonate the banks because the telephone security protocol adopted by almost every bank focuses on the customer proving that they are the customer, and makes no effort to prove that the bank is the bank.

6) In addition to this the telecomms companies allow unrestricted access to software for making spoof calls and fake calls, allowing the fraudster to display the bank's phone number. Most people are still do not know that they cannot trust the caller ID.

7) House purchase / deposit fraud

8) Recognising that paying the deposit on a house, or in some cases buying a house, is the highest value transaction that most people make, it still amazes me just how little protection the banks and the solicitors/conveyancers provide to their customers.

9) In several cases that I have dealt with the fraudsters were actually sending emails through the solicitors email system, meaning that they looked completely genuine.

10) Several banks do not specifically identify payments as being for house purchases, and do not, therefore, present the correct warnings or fraud prevention advise.

11) All solicitors/conveyancers should be required to put their bank details on a national register, managed by the SRA, and all banks should identify 'property' transactions and validate them against the register.

12) **Investment fraud** (sometimes linked to crypto-currencies).

13) I recognise that detecting investment fraud is challenging. Investors are not expecting returns, or correspondence, for months or years after making the payments.

14) A significant responsibility for preventing investment fraud lies with the receiving banks who are failing to implement and operate effect KYC and AML processes.

Q2. What role can technology and tech companies play in combatting fraud?

15) Prevent unauthorised spoofing of phone numbers and text message IDs so that people can be sure that phone calls and text messages come from the genuine organisation.

ACTION TO TACKLE FRAUD

Q5. How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

16) The current structure for policing fraud is largely ineffective, with the exception of the DCPCU and one or two teams of dedicated officers in local forces.

17) The absence of a coherent strategy is demonstrated by the HBOS Reading case. This major national fraud was successfully investigated and

prosecuted by Thames Valley Police only because of the commitment of the then Police and Crime Commissioner, Anthony Stansfeld. It cost Thames Valley Police nearly £7m and over 3 years work to prosecute this case, only £2m of this will be recovered from the Home Office, according to a report by Anthony Stansfeld.

18) Action Fraud is the wrong title for an organisation that is no more than a National Fraud Reporting Centre. The public perception is that they do nothing with the reports that they receive and I struggle to disagree with this sentiment.

19) The NFIB may, on occasions, share information with the banks, but I have to ask how much notice the banks take of it? In 'Gary's' case, the NFIB wrote to the bank, warning them that an account might be being used for fraud. The bank clearly ignored the warning, and the account was not shut down for another two months, during which time nearly £200k of stolen money went through it. It was only shut down when Gary reported the fraud to his bank, and they notified the receiving bank.

Q6. Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not?

20) No!

21) As stated above, it is widely accepted that 40% of all crime is economic but less than 2% of police budgets is spent fighting it, and there is a woeful lack of experienced officers and civilian staff dedicated to the task.

22) I ask if the SFO should be disbanded, with its activities taken over by the National Economic Crime Team (NECTs) (see below).

23) Serious consideration should be given to the development of a dedicated Economic Crime Prosecution Service, established in line with the NECTs.

Q8. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

24) GDPR is used by the banks to obstruct investigations by victims of crime.

25) Paragraph 5(3) of Part 1, Schedule 2, of the DPA 2018 specifically allows for the disclosure of personal data where disclosure of the data: (a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings).

26) A victim of fraud should be allowed to access the personal details of the account holder of the account into which they paid their money, so that they can issue civil proceedings against that person, but the banks adamantly refuse to disclose the information, citing GDPR.

27) I am concerned that they do this because disclosure would reveal failings in their KYC and MLA compliance.

Q9. What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

28) If the banks spent even a modest proportion of the advertising budget and creative resources on consumer education, then it could have a real impact on preventing fraud from taking place.

29) But, and this is big but, the banks needs to be transparent about their systems and processes.

30) For example, when the banks (reluctantly) implemented Confirmation of Payee they almost did it secretly. Why? I believe that this was because they didn't want to admit that they hadn't been validating, or even using, the Payee name since 2008 when the Faster Payment System was introduced. The use of the "unique identifier" (the combination of the sort code and account number) as the sole reference for making payments is buried in the banks' T's&C's. Most banks even ignored the Bank of England rules for making CHAPS payments by not telling the customer that although the customer had to check that the Payee name was exactly correct, the bank would ignore it when making the payment.

LEGISLATIVE REMEDIES

Q11. Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions?

31) In 2019 the major banks agreed a voluntary code of conduct known as the CRM Code. The shockingly low level of reimbursement by the banks and the exceptionally high complaint uphold rate by FOS, clearly demonstrates that the banks are widely flouting their obligations under the Code.

32) The Code clearly sets standards for "Effective Warnings" but the banks consistently decline to tell the customer the wording of the warnings that the customer is meant to have ignored. The lack of transparency results in a lack of accountability.

33) I am currently assisting a number of groups of people where the Police have arrested the fraudster, but the banks are insisting that the cases are "private civil disputes", which fall outside of the CRM Code, and not "fraud" which they would have to consider for reimbursement under the Code.

34) In light of the unacceptably poor compliance with the voluntary CRM Code I believe that regulation is required to make the banks implement six systems and processes that could, and should, have been developed and

implemented in the past, and which would have prevented more than £2bn of APPFraud in the last 7 years.

34.1) Confirmation of Payee to be implemented by every Payment Service Provider, including banks, building societies, electronic money institutions and authorised payment institutions.

34.2) 24-Hour Payment Delay on all high value payments made by personal customers to new payees, with an option to have a 24-hour delay on all high value payments, even to existing payees.

34.3) Second-Party Notification, under which the customer would nominate a Second Party, e.g. a close family member, friend or carer, to receive copies of all messages sent by the bank. This would alert them to possible fraud.

34.4) Bank Identification, under which the banks would be required to prove that they are the bank, in the same way that they require the customer to prove that they are the customer.

34.5) Disclosure of Payee details to allow victims of fraud to pursue civil actions against the fraudster.

34.6) Active Account Monitoring of inbound transactions to detect and freeze suspicious receipts.

Q12. Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

35) The major barrier to prosecution fraudsters is catching them! (see Q6 and Q15)

Q13. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful?

36) No deterrent is effective if you cannot catch the criminals in the first place.

37) I would like to see fraudsters required to face their victims and hear what they have done to them. The fraudsters need to know that their crimes are not victimless. They need to know that ruin people's lives.

BEST PRACTICE

Q15. Can you suggest one policy recommendation that the Committee should make to the Government?

Economic crime will only be tackled effectively through the establishment of a fully funded National Economic Crime Team (NECT), located across nine regional centres, appropriately resourced by specialist Police and civilian staff, such as forensic accountants, on permanent appointments, and supported by a dedicated Economic Crime Prosecution Service, and with a regulatory

requirement for the banks to actively co-operate with Police investigations, rather than hiding behind GDPR.

22 April 2022