Select Committee Evidence
Public Accounts Committee: The Growing Threat of Online Fraud

Which? is the largest consumer organisation in the UK with more than 1.5 million members and supporters. We operate as an independent, apolitical, social enterprise working for all consumers and funded solely by our commercial ventures. We receive no government money, public donations, or other fundraising income. Which?’s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people’s lives fairer, simpler and safer.

Summary

1. Which? welcomes this opportunity to submit evidence to the Public Accounts Committee’s inquiry on The Growing Threat of Online Fraud. As noted by the Committee, the latest figures from the Office for National Statistics (ONS) show the increasing scale of the problem with approximately one in six of all estimated crimes in England and Wales being a case of fraud that was committed online.

2. Which? research from September 2017 revealed that four in ten (40%) people believe that financial fraud and scams should be one of the top three consumer priority issues for Government.

3. Which? welcomed the Government’s commitment to tackle fraud in the UK by establishing the Joint Fraud Taskforce in February 2016. Given the nature of fraud it is vital that there is a coordinated approach across Government, law enforcement and the financial industry to identify and combat the threats to consumers.

4. However, 18 months on from its creation, we are concerned about the lack of transparency both in terms of what the taskforce is working on, but also importantly what progress it has made to date.

5. Earlier this year the National Audit Office published its report into online fraud, which shared Which?’s concerns about this lack of transparency and recommended that the Government should publish information on the Joint Fraud Taskforce’s performance and future plans. It also recommended that the Government “identify and implement suitable
accountability arrangements, including within the Joint Fraud Taskforce, so that the responsibilities of all partners for preventing and reducing online fraud are clear”.

6. In September 2016, Which? highlighted the lack of protection for consumers who make Authorised Push Payments (APP), also commonly referred to as bank transfers or Faster Payments. Despite consumers making over 70 million of these transactions a month, unlike with other payment types, such as credit or debit cards, people who are tricked into transferring money to a fraudster currently have no legal right to get their money back from their bank. We submitted a super-complaint to the Payment Systems Regulator (PSR) on this issue⁴.

7. The PSR found that data available on the scale and types of APP scams is of poor quality. However, it acknowledged the considerable consumer harm caused by bank transfer scams, identified evidence to suggest that the scale of the problem may be significant, and concluded that the prevalence of these scams is likely to increase. The regulator agreed that banks could to do more to protect their customers: they needed to improve the way they respond to bank transfer scams, and do more to identify fraudulent payments. It proposed a package of work for the industry to take forward, including improving the way industry responds to bank transfer scams, and doing more to identify fraudulent payments⁵.

8. The regulator will publish a progress report in November 2017. Which? wants to see clear progress on the measures that the PSR tasked industry with improving. The regulator must also provide an update on the progress being made to swiftly introduce Confirmation of Payee, and set out proposals to ensure consumers are not left out of pocket when they fall victim to a bank transfer scam.

9. The methods used by scammers are increasingly sophisticated, making it more challenging for consumers to equip themselves with the necessary tools and information to protect them.

Joint Fraud Taskforce

10. Which? supported the formation of the Joint Fraud Taskforce in 2016. However, we are concerned that it is yet to demonstrate what it has achieved, and we agree with the NAO that whilst the creation of the Joint Fraud Taskforce was a positive step, without a clear update on what it has achieved “it is hard to judge that the response to online fraud is proportionate, efficient or effective.”

11. Which? has called on the Government to publish an update on the progress of the Joint Fraud Taskforce and outline what action it would urgently take to safeguard consumers from scams. In our Consumer Agenda for Government⁶, published in April 2017, Which? called on the Government to ensure that the Government’s Joint Fraud Taskforce sets out an ambitious agenda for tackling fraud and scams in the next Parliament. However, six

---

¹ https://www.which.co.uk/policy/money/349/payment-method-surcharges-which-super-complaint
months on from this, three months since the NAO’s report and 18 months after it was established, it is not clear what progress the taskforce has made or what areas it has identified that it will tackle.

12. In May 2016 Which? launched its ‘Safeguard us from Scams’ campaign, calling on the Joint Fraud Taskforce to examine whether companies are taking enough responsibility when their customers are defrauded, as well as investigate what improvements should be made to the processes, systems and practices firms use to prevent fraud. Which? also asked them to recommend, by the end of the year, how companies can better protect their customers from fraud.

13. In the last six months alone, Which? has highlighted the increasing types of scams that consumers are either at risk of, or in many cases have already fallen victim to. In May this year, a Which? investigation highlighted the risks to consumers looking to secure a rental property through various popular sites. We were aware that consumers were falling victim when a listing encouraged the user to make a bank transfer outside of many of the sites secure systems that offer additional protection if things go wrong. Our investigation into this found that on several of the most popular sites we would have been able to post fake listings and include information about how to be contacted outside of the secure system.

14. Which? also analysed the data of cases reported to Action Fraud to identify particular fraud hotspots across England and Wales where people were more likely to report being victim of a particular scam. Our analysis found people in Dorset were more likely to report being victims of Computer viruses, malware or spyware, whilst in Northamptonshire there were a great number of reports of online shopping and auction scams. In the October edition, Which? Money investigated the ease in which some fraudsters are able to open online bank accounts in order to use them to facilitate scams. The research showed how easy it would be for a fraudster to gather the information needed to build a profile of an individual who they would use to open an account.

15. Also in October, Which? Computing magazine published a review of the various online scams consumers are likely to encounter on social networking sites such as Facebook. The article highlighted common scams including ‘like farming’ where emotive posts are designed to go ‘viral’ collecting ‘likes’ which fraudsters then use to mine and sell the contact details of people who have responded to the post to marketing companies, as well as more recognisable scams involving fake goods and sales.

16. These examples are a snapshot of the types of fraud facing consumers today, across a wide range of sectors. They demonstrate both the growing scale and broad scope of the scams that consumers have to navigate daily. It is clear that as new technology and services develop to better suit consumer’s need, such as swifter access to bank accounts online or the ability to easily find holiday accommodation, fraudsters will find loopholes to exploit vulnerabilities and target victims.

---

4 The Great Holiday Rental Scam, Which? Travel, May 2017
5 Are you living in a fraud hotspot? Which?, July 2017
6 ID theft: how fraudsters could use your details to open bank accounts, Which? Money, October 2017
7 Facebook scams, Which? Computing, October 2017
17. Which? also recently conducted research into how easy it is for fraudsters to hijack existing systems used by banks to communicate with its customers that they trust. Using easily available online tools, known as text ‘gateways’, that enable legitimate companies to send thousands or even millions of messages at a time, for less than a penny a text, fraudsters are able to target consumers whose data they have obtained. Crucially, these gateways allow the user to replace a phone number with a short name (e.g. Barclays), which will appear when they use the number to send texts. However, this same technology is available to fraudsters and whilst the providers of those services do attempt to check use is lawful, fraudsters have to still managed to gain access to it. This means the fraudster can also replace a phone number with a short name and Which? research found that if the individual has already received genuine texts from a company of that name, and the spelling matches up, the phone will group fraudulent messages in with them. (Please note, this research has not yet been published, and is under embargo until 18th October 2017. The full research will be published in the November edition of Which? magazine.)

18. This is precisely the type of issue that the Joint Fraud Taskforce should be working with law enforcement, the banking industry, and the telecoms sector to address. Indeed, when it was launched, one of the streams of work that the taskforce was due to address was “tackling systemic vulnerabilities - removing the weak links in systems and processes, which fraudsters can exploit”. Without the publication of a progress report by the Joint Fraud Taskforce, it is unclear what action has been taken and which systematic vulnerabilities the taskforce has focused on.

19. Only by adopting a coordinated approach to address these issues will consumers be confident that the messages they receive are genuine. Failure to tackle systematic vulnerabilities such as the example set out above could lead to a lack of consumer trust in services and therefore a knock on effect on innovation and competition if consumers refuse to use them.

**Authorised Push Payment Scams**

20. Which? is concerned that unlike with other payment types, such as credit or debit cards, people who are tricked into transferring money to a fraudster currently have no legal right to get their money back from their bank.

21. Despite a lack of official industry data recording just how prevalent this type of fraud is Which? has seen evidence that this is a significant problem.

22. In 2016, we collected evidence directly from consumers via an online scams reporting tool and have heard case studies from over 600 people explaining how they, or someone they knew, had lost over £5.6 million to bank transfer scams. Most people lost on average £1,200, but a small number of losses were in excess of £200,000\(^8\).

\(^8\) Which? launched its scams reporting tool on Friday 4th November. Statistics in this release are correct as at 16th November 2016, after the tool had been active for 13 days. Total uses of the tool were: 31,018; Of which reports by individuals affected by
23. In May 2017, Which? published research that found that of the one in 10 (8%) people in the UK who either knew someone or had fallen victim themselves to bank transfer fraud, more than half (54%) had been victims in the last six months⁹.

24. Individual losses can cause significant distress and as shown involve large, life-changing sums of money. Increases in maximum transfer limits, and the number of faster payments being made, have increased the scale of potential harm.

25. Our super-complaint detailed a number of failings that meant consumers who fall victim to this type of scam are likely to be left out of pocket. These included inconsistent processes and availability for consumer to be able to report a case of APP fraud, as well as the lack of data sharing between banks in order to better protect consumers and the absence of any recorded statistics demonstrating the level of this type of fraud.

26. Which? is concerned that the PSR has not yet gone far enough or required swift enough action, and the result is that consumers will continue to lose millions of pounds to fraudsters. Although we have some indications from industry and the regulator that this continues to be a priority and progress is being made, the latest statement¹⁰ from the PSR to mark the one year anniversary of the super-complaint indicated that an update on what has been achieved will not be published until November 2017.

Which?
October 2017

---

¹⁰ Scams research: Populus, on behalf on Which? spoke to 2,117 nationally representative UK adults via an online poll between the 3rd and 4th May 2017.