Which?, 2 Marylebone Road, London, NW1 4DF
Date: 8 May 2018
Response by: Which?

Written evidence to the Treasury Committee inquiry into the effect of economic crime on consumers

About Which?

Which? is the largest consumer organisation in the UK with more than 1.7 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 the opportunity to respond to the Treasury Committee inquiry on Economic Crime and supports the committee's decisions to focus one strand of the inquiry on economic crime as it affects consumers.

2. The scale of fraud faced by consumers means tackling fraud should be a top priority for Government. Which? research shows that four in ten people believe financial fraud and scams should be one of the top three consumer priorities for Government.

3. Which? regularly provides information and advice on the different types of scams that consumers are being targeted with. Over the past year, this includes fake listings in the rental market which encourage consumers to contact individuals outside of a secure system, and fraudsters using fake texts to communicate with bank customers. As scammers will continue to adapt their methods the Government must work together with regulators and businesses from all sectors to ensure that its preventative tactics and actions keep pace with the new technology and changing methods used by scammers.

4. Currently consumers are not adequately protected for scams involving authorised push payments (APPs). In September 2016, we submitted a super-complaint[1] to the Payment Systems Regulator (PSR), highlighting that when people are subject to sophisticated scams and are tricked into transferring money to fraudsters via bank transfer, banks do not provide the levels of protection that they could – and that they typically do provide for other types of payment.

5. Which? welcomes the work being undertaken by the Payment Systems Regulator (PSR) and industry on combating APP fraud. In particular, it is important that the proposed contingent reimbursement model is delivered effectively, and the plans outlined by the Payments Strategy Forum for 'Confirmation of Payee' verification are introduced swiftly.

---

[1] https://www.which.co.uk/policy/consumers/347/consumer-safeguards-in-the-market-for-push-payments-which-super-complaint

The scale of fraud faced by consumers means tackling fraud should be a top priority for Government

6. Which? research from September 2017 revealed that four in ten people believe financial fraud and scams should be one of the top three consumer priority issues for Government. The latest figures from the Crime Survey for England & Wales for show that there were 3.2 million incidents of fraud in England and Wales in the year ending December 2017. Of these incidents, 2.3 million were bank and credit account fraud and a further 813,000 were consumer and retail fraud. Incidents of fraud accounted for 30.5% of crime recorded by the survey.

7. Which? conducted research into incidents of APP fraud in May 2017 and found that 3% of people said they had made a bank transfer into a fraudulent account; among people ages 18 to 34 that figure was 8%.

8. UK Finance data appears to show that the amount lost to APP scams has actually increased in the last six months. UK Finance figures show that a total of £236.0 million was lost to APP scams in 2017. £101.2 million was lost to this type of fraud in the first six months of 2017, and £134.8 million in the second six months. Financial providers were only able to return £60.8 million (26%) of the authorised push payment scam losses in 2017.

9. In 2016, Which? collected evidence directly from consumers via an online scams reporting too and 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. Individual losses can cause significant distress and can 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.

Over the last year Which? has highlighted a number of scams that consumers are being targeted with. Our investigations highlight that the nature of scam is varied and evolving and so Government, regulators and business must work together to keep pace

10. The nature of scams is changing with technology. Online scams and fraud are on the rise and scammers are becoming increasingly sophisticated. Below are examples of some of the scams highlighted by Which? over the past year.

11. Holiday Rental Scams **-** In May 2017, 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[2].

[2] The Great Holiday Rental Scam, Which? Travel, May 2017

12. Imposter Bank Accounts - In October 2017, a Which? Money investigation was conducted into the ease with 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[3].

13. Scam Texts - In November 2017, Which? Money 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 fraudster to replace a phone number with a short name (e.g. the name of a bank), which will appear when they use the number to send texts. 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[4].

14. The nature of scams is varied. Scammers will adapt their methods and evolve their techniques to counter whatever measures are introduced. The Government must therefore ensure that its preventative tactics and actions keep pace with the changing methods used by scammers. This should include the Government working together with regulators and businesses from all sectors to introduce new technology, take enforcement action, and align businesses' incentives to ensure consumers are protected from scams.

15. There is a need for a coordinated response to fraud. While Which?'s super-complaint on APP fraud focused on the responsibility of the banking industry to better protect consumers, there is more that other sectors could also do. In the case of number spoofing, for example, telecoms companies and Ofcom will work with banks to seek solutions to close the loopholes fraudsters exploit. It is important that wherever a system's vulnerabilities are exploited, the most appropriate bodies, with control over improving the situation, takes responsibility and work together. New technology could also help tackle this type of scams. In January 2018, HMRC reported that that it had 'stopped thousands of taxpayers from receiving scam text messages, with 90 percent of the most convincing texts now halted before they reach their phones.'

Currently consumers are not adequately protected for scams involving authorised push payments (APPs), so it's vital that the Payment Systems Regulator's proposed contingent reimbursement scheme ensures that consumers are not left out of pocket when falling victim to these sophisticated scams.

16. Our super-complaint called for greater consumer safeguards in the market for authorised push payments. We suggested that placing more liability on banks for the losses from APP scams would create efficient incentives for banks to develop systems to better manage risks, through identifying and checking high risk payments while maintaining the benefits of

[3] ID theft: how fraudsters could use your details to open bank accounts, Which? Money, October 2017
[4] Text Alert, Which? Money, November 2017

Faster Payments (and not reducing liability on consumers who had been grossly negligent or acted fraudulently).

17. The current approach, overtly focused on education and awareness raising, places too much responsibility on consumers to identify scams and take action to protect themselves. Consumers are not best placed to identify or manage the risk, in comparison to the banks involved, who have access to more transactional data, and information about the payees, and who are likely to be more aware of the type of attempted scam being perpetrated. Responsibility for preventing these scams should be allocated to those who are best able to manage the risk of scammers using bank accounts and payment systems to facilitate their scam.

18. Whilst there is value in making consumers more aware of actions they may be able to take to guard against APP fraud, education or awareness raising campaigns alone are unlikely to have a significant impact on reducing the number of people who fall victim to this type of fraud, compared to other interventions that banks could make.

19. As fraudsters' methods develop and become increasingly sophisticated, any education campaign would need to be constantly renewed and constantly re-delivered to reach consumers, who would constantly need to act on this new information.

20. The super-complaint highlighted inconsistent processes and availability for consumers 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. In response, the PSR agreed that banks could to do more to protect their customers and proposed a package of work for the industry to take forward: developing common standards to collect data, an approach to responding to instances of reported scams, and proposals for better sharing of information.

21. Which? welcomes the work that the PSR and industry has undertaken since our super-complaint towards improving the detection, prevention, and response to scams.

22. In particular, we welcome the commitment to introduce a contingent reimbursement model. The scheme must provide an effective way for consumers to be reimbursed, and must cover all applicable PSPs. Which? is part of a steering group formed by the PSR to design the code that will underpin the reimbursement scheme.

23. Which? also welcomes the plans outlined by the Payments Strategy Forum for 'Confirmation of Payee' which will allow bank customers to verify details of the payee before money is transferred. The system will be available from December 2018 and, it is critical that all banks quickly act to introduce this measure to help protect their customers from scams.

24. At the same time, it is important that work to improve repatriation of funds continues, and progress is made to improve data sharing between banks. If banks need further guidance on what data they are able to share, then regulators should seek to provide it. In addition, if banks feel unable to take action to protect their customers due to fear of breaching existing regulations, then interim solutions, or regulatory guidance, should be explored that might give banks some form of protection in good faith when they are explicitly acting to protect

their customers and prevent fraud. Which? would also support calls to introduce new legislation that allows the financial sector to more easily share information to prevent and detect all types of economic crime, as this could help prevent fraud and better protect consumers.

25. New technologies, such as open banking, have the potential to give consumers greater control over their money and to increase innovation, however they also create more opportunities for fraudsters. The introduction of open banking will potentially see incidents of APP fraud increase as consumers make use of the technology to make more direct payments, making the work on a contingent reimbursement scheme and 'Confirmation of Payee' increasingly important for the protection of consumers.

For more information, contact Richard Piggin, Head of External Affairs: richard.piggin@which.co.uk

May 2018