House of Commons

Treasury Committee

# Economic Crime: Consumer View

## Third Report of Session 2019

*Report, together with formal minutes relating to the report*

*Ordered by the House of Commons to be printed 22 October 2019*

**HC 246**
Published on 1 November 2019
by authority of the House of Commons

## The Treasury Committee

The Treasury Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of HM Treasury, HM Revenue and Customs and associated public bodies.

### Membership

Mel Stride MP (Chair) *(Conservative, Central Devon)*

Rushanara Ali MP *(Labour, Bethnal Green and Bow)*

Mr Steve Baker MP *(Conservative, Wycombe)*

Colin Clark MP *(Conservative, Gordon)*

Mr Simon Clarke MP *(Conservative, Middlesbrough South and East Cleveland)*

Charlie Elphicke MP *(Independent, Dover)*

Alison McGovern MP *(Labour, Wirral South)*

Catherine McKinnell MP *(Labour, Newcastle upon Tyne North)*

Wes Streeting MP *(Labour, Ilford North)*

Alison Thewliss MP *(Scottish National Party, Glasgow Central)*

### Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

### Publication



Committee reports are published on the Committee's website at www.parliament.uk/treascom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

### Committee staff

The current staff of the Committee are Gail Bartlett (Second Clerk), Emily Buckland (on secondment from the Bank of England), Sarah Goodwin (on secondment from the Prudential Regulation Authority), Rachel Kift (on secondment from the National Audit Office), Dan Lee (Senior Economist), Gosia McBride (Clerk), Aruni Muthumala (Senior Economist), Matt Panteli (Senior Media and Policy Officer), Yasmin Raza (on secondment from the Financial Conduct Authority), Anne Stark (on secondment from HM Revenue & Customs), Baris Tufekci (Committee Support Assistant), Adam Wales (Chief Policy Adviser), Maciej Wenerski (Senior Committee Assistant), and Marcus Wilton (Senior Economist).

# Contents

# Summary

This report is the second we have published on economic crime in the UK. Our first inquiry—*Economic Crime - Anti-money laundering supervision and sanctions implementation*—was focused on money laundering, terrorist financing and sanctions in the UK as well as the regulatory and legislative landscape. This inquiry has focused on the scale of economic crime faced by consumers, ways that financial firms are combating economic crime, how economic crime is investigated, and consumer's rights and responsibilities.

In the first half of 2019 over £600 million was stolen from consumers by fraudsters. It is a serious problem, with scams getting ever more sophisticated, from so-called "romance fraud" to posing as a consumer's internet provider. Authorised push payment (APP) in which a consumer is conned into processing a payment to an account controlled by a criminal is a new and growing problem.

In the first half of 2019, the industry prevented £820 million of unauthorised fraud. One key area of prevention, due to begin implementation soon, is Confirmation of Payee. To date fraudsters have relied on the account name not being matched to convince consumers to transfer money. This continued despite banks knowing this was a weakness in the system. The new system will match actual account names with those provided by consumers and flag any differences. While it will not solve economic crime alone, it is part of the solution. Further delays to implementation should not be allowed, and the regulators should look to use statutory powers if financial firms are not ready by the March 2020 deadline.

Fraudsters often use high pressure tactics to convince consumers to transfer money, which do not allow a consumer time to consider if they are being defrauded. We recommend that all initial payments between accounts are subject to a 24-hour delay.

There have been positive technological developments which allow financial firms to track fraudulent transactions across the banking system. However, legislation lags behind, making recovery of these funds difficult. The Government should review recovery of stolen funds legislation to ensure it is fit for purpose. The FCA should set tight deadlines for financial firms to block accounts receiving stolen funds once suspicious activity has been identified.

The Contingent Reimbursement Model, which came into effect in May 2019, provides financial firms with a clear framework under which they should reimburse. We understand that the Code's voluntary basis allowed it to be introduced quickly. However it should now be made compulsory.

Whether or not a consumer is reimbursed also comes down to whether they are deemed to be 'grossly negligent'. The lack of definition of this term has led to inconsistencies across the sector and we recommend the regulators define this promptly. The regulators should require financial firms to provide consumers with clear guidance on what they expect of their customers in light of that definition.

We heard that there had been a lack of resourcing allocated to investigating economic crime. A national fraud strategy is only just being implemented, which will include a commitment to improve the police response to fraud. This has taken far too long and we expect a Government update within six-months of publication of this report.

The Government should require all frauds to be reported by the financial sector. It must also ensure consumers reporting fraud are told clearly how their reports will be used. The reported attitudes of staff at Action Fraud towards victims are unacceptable and the Government must set out what it has done to address this issue.

# Introduction

## Conduct of the inquiry

1. On 29 March 2018, we launched an inquiry into Economic Crime. We announced that the inquiry would be organised into two strands:

- Anti-money laundering and the sanctions regime. The Committee would examine the scale of money laundering, terrorist financing and sanctions in the UK, the current regulatory and legislative landscape, and how individuals, firms, and the wider economy have been impacted by these regimes and the implementation of them.

- Consumers and economic crime. The Committee would scrutinise the scale and nature of economic crime faced by consumers, particularly retail bank consumers, the effectiveness of financial institutions in combatting economic crime, and the security of consumers' data.[1]

2. We published a Report covering the anti-money laundering and the sanctions regime in March 2019.[2] The Government responded in May 2019.[3]

3. This Report covers consumers and economic crime. While we again examine the law, this time we focus on how legislation affects consumers, both directly and indirectly, who have experienced financial crime during their interactions with financial services firms. We define financial services firms as banks, building societies and payment system providers.

4. As well as receiving wide ranging written evidence, we held the following oral evidence sessions:

- 27 November 2018—Richard Piggin, Head of External Affairs, Which?; Richard Emery, Independent Fraud Investigator, 4Keys International.

- 8 January 2019—Police Commander Karen Baxter, Police National Coordinator for Economic Crime, City of London Police; Detective Chief Superintendent Peter O'Doherty, Head of Crime and Cyber, City of London Police.

- 13 February 2019—Stephen Jones, Chief Executive, UK Finance; Susan Allen, Head of Retail Business Banking, Santander UK; Chris Rhodes, Chief Product and Propositions Officer, Nationwide Building Society.

- 2 April 2019—Panel 1: Mark Tingey, Head of Financial Crime Operations, Metro Bank; Panel 2: Ruth Evans, Independent Chair, Authorised Push Payments Scams Steering Group; Richard Lloyd, Advisor, Authorised Push Payments Scams Steering Group.

1 'Economic crime inquiry launched', Treasury Committee press release, 29 March 2018

2 Treasury Committee, 'Economic crime - Anti-money laundering supervision and sanctions implementation', 8 March 2019

3 Treasury Committee, 'Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation', 7 May 2019

- 15 May 2019—Megan Butler, Executive Director, Investment, Wholesale and Specialists Division, FCA; Chris Hemsley, Co-Managing Director, Payment Systems Regulator; Mark Steward, Executive Director of Enforcement and Market Oversight, FCA.

We would like to thank all those who provided written and oral evidence during this phase of the inquiry.

# 1 The type and scale of economic crime affecting consumers

5. Fraud "is now the second most common crime type in England and Wales, with nearly every individual, organisation and type of business vulnerable to fraudsters."[4] Greater Manchester Police Force defines fraud as "the volume crime of the 21st Century"[5] and the Financial Ombudsman Service recently told us it had seen "significant growth" in economic crime cases.[6]

## Types of economic crime affecting consumers

6. There are two main types of economic crime affecting consumers: authorised and unauthorised payment fraud. UK Finance, a representative body for the banking and finance industry, defines these as follows:

> Authorised fraud: In an authorised push payment (APP) fraudulent transaction, the genuine customer themselves processes a payment to another account which is controlled by a criminal.
>
> Unauthorised fraud: In an unauthorised fraudulent transaction, the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party.[7]

7. We heard evidence about specific scams which illustrate these two different categories of fraud. Authorised fraud (or APP Fraud) could include

- asking for temporary use of a bank account to transfer funds;[8]
- romance fraud where dating sites are used to develop a sham relationship where cash is eventually requested;[9] and
- holiday letting scams where consumers pay fraudsters for what turns out to be a fake listing.[10]

8. These examples all require the consumer to authorise the payment themselves—the fraudster does not take over the consumer's bank account.

9. With unauthorised fraud, the fraudster does take control of the consumer's bank account and as such the consumer is very often unaware the payment has been made. An example given to us was when a consumer receives a phone call from a fraudster posing as their internet provider. The scammer convinces the consumer to give them remote access to their computer, allowing the scammer to access their bank accounts.[11]

4 HM Government, Economic Crime Plan 2019–22, July 2019, Page 11
5 "Fraudster poses as Jason Statham to steal victim's money", BBC News, 29 April 2019
6 Treasury Committee, Oral evidence: Independent Review of the Financial Ombudsman Service, HC1400, 22 January 2019, Q213
7 UK Finance, 'Fraud the facts 2019', March 2019, p7
8 Q583
9 Q583
10 Q550
11 Q583

## Scale of economic crime affecting consumers

10. UK Finance collates figures on the levels of authorised and unauthorised fraud each year. In the first half of 2019, £408 million was stolen by fraudsters via unauthorised fraud and £208 million via authorised fraud.[12] The total figures reported for 2018 were £844 million stolen via unauthorised fraud, and £354 million via authorised fraud, while in 2017 £731 million was stolen in unauthorised fraud and £236 million in authorised fraud.

11. There are also significant volumes of unauthorised fraud prevented by financial services firms. UK Finance report that banks and card companies managed to prevent £1.66 billion of unauthorised fraud in 2018, the equivalent of £2 in every £3 of attempted fraud.[13] In the first half of 2019 the industry prevented £820 million of unauthorised fraud.[14]

12. It is difficult to get an accurate understanding of the scale of consumer economic crime. UK Finance has cautioned that the authorised fraud figures are not directly comparable year on year as there are now more banks reporting and greater clarity around what an APP scam is.[15] Megan Butler, Executive Director, Investment, Wholesale and Specialists Division at the Financial Conduct Authority (FCA), told us that:

> There are a lot of different statistics out there that try to size this problem in different ways, but the consistent message that comes through, although the numbers do not necessarily reconcile terribly well, is that this is a significant problem, and it is growing.[16]

13. The Government's Economic Crime Plan, published in July 2019, states that "Economic crimes can involve complex methodologies that are continuously changing as criminals and terrorists identify and exploit new vulnerabilities in society."[17] Megan Butler of the FCA told us that growth in economic crime was often linked to technological developments, which allowed scams to progress quickly.[18]

14. The speed at which economic crime can develop can be demonstrated by the FCA's 'Financial crime: analysis of firms' data' report. Published in November 2018, it did not mention APP Fraud.[19] This is because when the FCA designed the survey they relied on outdated categories of economic crime, established before APP Fraud became the significant scam it is now.[20]

15. **It is clear, both in terms of financial losses and in the variety of scams suffered by consumers, that economic crime is a serious and growing problem in the UK. Trends need to be identified quickly.** ***In order to ensure a clear picture of the scale and types of economic crime facing consumers, the FCA should publish data on economic crime within six months. It should evolve its data collection practices to ensure they allow for emerging trends, while still enabling year-on-year comparisons.***

12 UK Finance, 2019 Half year fraud update, 26 September 2019, p2
13 UK Finance, 'Fraud the facts 2019', March 2019, p7
14 UK Finance, 2019 Half year fraud update, 26 September 2019, p5
15 UK Finance, 'Fraud the facts 2019', March 2019, p41
16 Q839
17 HM Government, Economic Crime Plan 2019–22, July 2019, Page 22, para 2.1
18 Q839
19 FCA, Financial crime: analysis of firm's data, November 2018
20 Q842

# 2 Prevention

16. As methods for defrauding consumers continue to change and develop, financial services firms have been working with the Government and Regulators to prevent fraud. This has sometimes been at firms' own initiative and sometimes in response to pressure from regulators or consumer groups. In this chapter we consider both fraud prevention initiatives already being implemented and those still under consideration.

## Data sharing

17. Financial firms already use data sharing to help them identify criminal activity which could be occurring across multiple banks. Chris Rhodes, Chief Product and Propositions Officer at Nationwide Building Society, told us that there "is a huge amount of data-sharing"[21] with other institutions.

18. However, we also heard that there was potential for more information to be shared between different financial institutions to prevent fraud and that regulations were getting in the way. Susan Allen Head, of Retail Business Banking at Santander UK said:

> There is room for us to do more on data-sharing […] Anything that helps us in terms of regulation to enable more of that would be really helpful.[22]

19. Stephen Jones, Chief Executive of UK Finance, told us:

> We have previously asked Government for a new power to share information more widely across the sector and not to have […] a criminal burden of proof before we start to do that. That will enable us to track, trace and prevent in a much more effective way.[23]

He explained that UK Finance did not believe the criminal exemptions in the Data Protection Act[24] were clear enough to allow data sharing at the pace and extent needed:

> We proposed to Government a general power and safe harbour for banks to share information for the purposes of preventing and detecting all types of economic crime. We asked for that in the Criminal Finances Act, and indeed the FCA supported that call, but Government rejected it.[25]

20. When the Criminal Finances Bill was proceeding through Committee stages in 2016, Nausicaa Delfas, Director of Specialist Supervision at the Financial Conduct Authority, called for:

> The threshold for sharing information to be lowered, so that institutions can share information when they see unusual activity and not just when they actually have enough information to have a suspicion.[26]

21 Q663
22 Q663
23 Q689
24 Data Protection Act 2018
25 Q720
26 Public Bill Committee, Criminal Finances Bill (Second sitting), 16 November 2016, col 41

This request was not implemented, though the Act does permit financial firms to share information under certain conditions if there is a suspicion an individual is involved in money laundering.

21. The concern around the ability of firms to share data was echoed by Police Commander Karen Baxter, the Police National Coordinator for Economic Crime at the City of London Police:

> Probably one thing [that could help] is around that facilitation of data sharing. […] GDPR has just put a framework around that. […] Perhaps it has slowed, in some cases, the exchange of that information.[27]

22. The Government sees data dating sharing as an important part of the fight against economic crime. Its *Economic Crime Plan 2019–22* says that:

> No one agency or organisation has the information, intelligence or data necessary to combat economic crime alone. This can only be achieved by agencies and organisations having the appropriate powers, gateways, frameworks and culture in place to facilitate the effective, appropriate and targeted sharing and use of information.[28]

23. In order to achieve efficient data sharing between firms the Government has set a commitment for a "public-private working group" to be set up which is "focused on information-sharing for economic crime purposes."[29] This working group will include the Home Office, HM Treasury, UK Finance and the National Economic Crime Centre. HM Treasury has told us that the working group is at an early stage and is currently developing policy workstreams.[30]

24. **The Government has not been listening to concerns that data sharing requirements for financial services firms are too restrictive and unfit for purpose.** ***We welcome the establishment of the public-private working group. Its remit must include assessing whether the current data sharing requirements are fit for purpose. If not, the working group must make detailed proposals to reform those legal requirements including considering using existing subordinate legislation-making powers under the Data Protection Act 2018 to amplify or clarify exemptions in the Act. The group should report to us every six months on progress made.***

## Blocking accounts receiving stolen funds

25. Financial services firms work together to track where stolen money goes once it is within the financial system. Susan Allen of Santander UK told us that Santander had invested £100 million in 2018 into combatting economic crime and that once a fraudulent account was identified, they were able to look for linked computers and mobile phones to see which other accounts were also being accessed via those devices.[31]

27 Q582
28 HM Government, Economic Crime Plan 2019–22, July 2019, p26, point 3.2
29 HM Government, Economic Crime Plan 2019–22, July 2019, p28, Action 6
30 HM Treasury (ECR0097)
31 Q687

26. Accounts holding money fraudulently obtained are reported to financial firms by the police and consumers. We questioned Megan Butler of the FCA on media reports that some bank accounts were still receiving funds eight weeks after the bank had been told they were receiving stolen funds. She told us that "[firms'] systems are very different and their ability to spot it is very different at the moment." She did not believe setting targets for how quickly an account should be blocked from receiving new payments would be the best solution:

> Generally we want banks to exercise judgment and to be capable of responding properly. The difficulty with setting hard and fast rules around this is that they then work to the hard and fast rule and not necessarily as quickly as they should in some particular circumstances.[32]

27. Chris Hemsley of the PSR provided information on developments within the sector remarking that "everyone needs to act as quickly as possible" and that:

> One quite encouraging change that happened last year were the changes that were put in place to improve the way that banks talk to one another. They agreed standard ways of passing information to one another, which facilitated the receiving bank acting more quickly on these types of frauds.[33]

28. **We are concerned over the length of time some accounts used in economic crime remain active once intelligence has been received on their potential misuse. Whilst we understand that prescribed timeframes could delay how quickly banks act, the difference in time each bank takes to act creates weakness in the UK financial system. *The FCA should work with financial institutions to ensure consistency across the sector. We recommend that the FCA uses its powers to set a timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently.***

## Confirmation of payee

29. Confirmation of Payee (CoP) is a new element of protection when sending a payment via the Faster Payments Scheme and CHAPS.[34] At present when a payment is sent, the initiator of the payment must give the payee's name, account number and sort code. While the latter two are cross referenced and confirmed with the receiving bank, the payee's name is not.[35] CoP involves the name of the recipient being confirmed as well as the account number and sort code when a payment was made. Chis Hemsley, Co-Managing Director of the Payment Systems Regulator, told us how the system is intended to work:

> If there is a perfect match between the account number and the name, you would expect the transaction to go through much as it does today[…]. If you are setting up a new payee, that is when these checks particularly come in. […] If there is a close enough match, so that it is Mr Smith rather than Dr Smith, for example, that there would be a warning. It would go back to the customer and say, "Actually the name is this. Is this who you want to

32 Q866
33 Q864
34 Payment Systems Regulator, Confirmation of Payee Response to the first consultation and draft specific direction for further consultation, May 2019, para 1.6
35 Q536

> pay?" If there is not a reasonable match at all and it is quite far away from it, you would expect the sort of warning that asks the customer to contact the payee again, to get the details right and restart or initiate that payment.[36]

30. Customers will be able to use this system by March 2020 when it will cover the six largest banking groups and 90% of eligible payments.[37] No timetable yet exists for smaller firms getting onto the system, however this will be a focus for the Payment Systems Regulator (PSR) once the largest six are up and running. Originally the PSR had set a timetable of July 2019 for CoP to be operational, however their consultation led to the conclusion this timetable was too tight.[38]

31. The current lack of payee name check can lead to cases where consumers believe they are paying one person—and insert that name—but in reality are sending to a fraudulent account. Richard Emery, Independent Fraud Investigator, 4Keys International, explained:

> Most individuals are completely unaware of the fact that it is possible for a fraudster to change the bank details in an attachment to an email. They receive an invoice by email. They are expecting it and have no reason to question it, so they pay it; but the money goes to an account controlled by a fraudster.[39]

32. Issues caused by the lack of name matching were raised by Which? in a 2016 super-complaint to the PSR which focused on "highlighting that when people are subject to sophisticated scams and are tricked into transferring money to fraudsters via bank transfer […] banks did not provide the levels of protection that they could–and that they typically would provide for other types of payment fraud."[40]

33. When we asked about progress of confirmation of payee implementation, Stephen Jones of UK Finance, said that "it is quite a complex IT and process change."[41] He also discussed a competition rationale for a delay until a wider range of institutions were able to offer the technology to consumers:

> There is also the issue that we want a broad variety of payment service providers in the system. […] While the large and sophisticated institutions […] have the resource to do what is required internally, a number of the middle and smaller-sized institutions do rely on third parties to deliver a solution to implement. […] If we go too fast, we will end up with a two-tier system where […] customers are forced to make a choice between the big institutions and mid-sized and smaller-sized institutions.[42]

34. The delay in rolling out CoP to a wider range of institutions will have consequences. Mark Tingey, Head of Financial Crime Operations at Metro Bank, said that "the more participants there are, the more successful it is going to be."[43] Chris Rhodes of Nationwide

36 Q857
37 Payment Systems Regulator, Confirmation of Payee Response to the first consultation and draft specific direction for further consultation, May 2019, para 2.33
38 Payment Systems Regulator, Confirmation of Payee Response to the first consultation and draft specific direction for further consultation, May 2019, para 1.4
39 4Keys International (ECR0076)
40 Which? (ECR0044)
41 Q626
42 Q627
43 Q744

explained that this was because the system "requires [the sending bank] to send a message to [the receiving bank] and for them to confirm that it is the right account, it has to work both ways."[44] Therefore, if not all financial firms with customer accounts are part of the scheme the protection becomes less effective.

35. Susan Allen of Santander UK provided the following explanation of the complications around a seemingly simple change:

> Our customers make payments in lots of different ways […] we have to make changes in every single one of those channels; we have to make changes that link into the payment systems; and then we have to make changes to be able to receive messages in from the other banks and present them back to the customer in whatever channel the customer chooses.[45]

36. Mark Tingey of Metro Bank explained that the variety of data which could be used—such as using a second name instead of a first name, or businesses using holding company names—creates issues around matching the data.[46]

37. One of the concerns around CoP is spelling mistakes. We questioned Mark Tingey of Metro Bank on this, asking what the system would flag if 'independent' was spelt incorrectly with an 'a'. Mark Tingey explained to us that "an obvious spelling mistake" would not be flagged, however he also said that the system needs to be "sophisticated enough to identify a genuine mistake versus a clear fraud."[47]

38. Confirmation of payee was seen as a positive step towards combatting economic crime. Richard Emery, an independent fraud investigator , told us that "it will make a lot of difference when it comes in"[48] and Megan Butler of the FCA agreed that it would "play a significant part as an anti-fraud measure.[49] However, we were warned confirmation of payee would not be the whole solution to economic crime. Megan Butler warned us that "It is not going to be the only thing that will stop [economic crime]. We need to recognise that there are other things that banks need to do."[50]

39. **Confirmation of payee will not solve economic crime alone, and as such the onus will always be on financial firms to develop further methods and technologies to keep up with fraudsters.**

40. **The fact that banks were not previously confirming payees is a serious failure to protect customers from harm. Asking for such information but not using it would have created a false sense of security among some customers when sending payments. It might have been better for banks to not ask for this information at all if they were not going to use it for fraud prevention.**

44 Q629
45 Q627
46 Q745
47 Q746-Q747
48 Q537
49 Q856
50 Q856

41. ***We therefore recommend that Confirmation of Payee should be introduced as a matter of urgency. Every delay leaves more people vulnerable to falling victim to economic crime. If the implementation date of March 2020 begins to look in doubt, regulators should consider introducing sanctions, such as fines, to firms who have not met the deadline.***

42. **The arguments put forward that Confirmation of Payee implementation could be harmful for competition if large firms implemented before small ones, is without merit. Competition in the banking sector exists for the benefit of customers, not for the benefit of firms. Customers should not be put at risk of becoming victims of fraud, in order to protect slow adopting firms from implementing protections for their customers. *The Payment Systems Regulator should therefore ensure that all relevant firms can implement Confirmation of Payee by the end of 2020.***

43. **Subtle differences which might not be immediately obvious to many people, such as using 'soliciters' rather than 'solicitors', could represent a fruitful way for fraudsters to disguise fraudulent accounts as legitimate accounts, and therefore small inaccuracies should be flagged for consumers' own protection. *We recommend that spelling mistakes are flagged within the new Confirmation of Payee System.***

## Delaying Faster Payments

44. Faster payments are an instant transaction which are normally processed and sent within a number of seconds, without a recall or reversal system built in.[51] Clearly this is something customers appreciate, however there is a balance between speed and safety. Stephen Jones of UK Finance explained to us that when a criminal is moving money it is "often split very quickly and very intelligently in seconds and put into multiple accounts that sometimes go cross-border."[52] Caroline Wayman of the FOS told us that "[…] the money moves in seconds so recovery is very difficult. Prevention is the best thing […]."[53]

45. Within the Faster Payments scheme it is currently possible to delay a payment for up to two hours to undertake scanning to detect fraud.[54] Chris Rhodes of Nationwide Building Society told us how Nationwide use this function:

> We suspend and delay up to 1,000 payments a week to do further investigation before they leave the society. About one in 20 of those turn out to be fraud.[55]

46. The faster payments delay is to enable the providers to detect fraud. It does not allow customers to protect themselves. Some banks have tried to introduce a delay that would be applied by the customer themselves. Susan Allen told the Committee that such an approach has not been very successful:

51 Faster Payments, How do I make sure that I do not become the victim fraud?, accessed June 2019
52 Q689
53 Treasury Committee, Oral evidence: Independent Review of the Financial Ombudsman Service, HC1400, 22 January 2019, Q219
54 Q631
55 Q631

> Customers already have the choice to change the timings of their payments. […] on its own that is not really sufficient, because the fraudsters are quite sophisticated and they can convince the customer that they actually should not tick that box.[56]

47. Richard Emery, an independent fraud investigator, told us how in his experience, the speed of the financial system contributes to consumers falling victim to fraud:

> The vast majority of authorised push payment fraud and unauthorised fraud […] happens within 24 hours of […] the creation of a new payee.[57]

48. Richard Emery suggested how it could be possible to counter the speed in the system:

> From the moment I create a new payee, [the bank] are not to release any payment to that payee until after a clear 24 hours. In that time, please send me a text message, an email or phone me with an automated voice message, but tell me that I have created a payee.[58]

The benefit of such a system would be that in a high pressured situation where a fraudster is persuading the victim to transfer funds, the victim would have 24 hours after setting up that payment to reassess the situation. In the case of unauthorised fraud, the account holder would become aware that someone else had accessed their account to set up a payee.

49. **Fraudsters rely on the speed of the payment system to move money into a series of different accounts before a customer or a customer's bank are aware that a fraud has taken place. The speed of transactions make it difficult for banks to trace stolen money once a fraud has occurred. Very few first-time payments need to be received instantaneously. Very large payments will often be scheduled days in advance. Therefore, high-speed payments on first time payments could be made redundant with only a limited impact on consumers.**

50. ***We recommend a mandatory 24-hour delay on all initial or first-time payments, during which time a consumer about to be defrauded could remove themselves from the high-pressure environment in which they are being manipulated. All future payments to that same account could flow at normal speed to minimise inconvenience to customers. If a situation arose whereby an initial payment was needed instantly, a customer could ring their bank and additional checks could be carried out for the funds to be released.***

## Tackling Mule Accounts

51. All of the frauds previously discussed in this report require somewhere for the money fraudulently obtained to be deposited. One of the ways fraudsters do this is to use a money mule account. CIFAS (Credit Industry Fraud Avoidance System–a not-for-profit fraud prevention membership organisation) define a money mule as "an individual who allows their bank account to be used to move criminal funds […]."[59]

56 Q643
57 Q539
58 Q539
59 CIFAS, Fraudscape 2019, June 2019, p10

52. Mule accounts are a significant problem for the financial sector. Santander estimated that it closed about 900 accounts a month which were suspected of being mule accounts[60] and Nationwide shut 23,790 accounts over a three-year period which had proven criminal activity.[61] Metro Bank estimated that it shuts around 200 mule accounts per month which "received confirmed proceeds of crime."[62]

53. The latest figures from CIFAS' 'Fraudscape 2019'[63] report showed that money mules were a growing problem. It reported that in 2018 there were around 40,000 cases that "bore the hallmarks" of money mule activity, a 26 per cent increase on the previous year. CIFAS attributed the increase in money mules to the increasing difficulty in opening accounts via identify fraud (down 12 per cent in 2018 compared to 2017), making it often easier to recruit a new money mule to launder funds than opening accounts specifically for the fraud intended. The data also showed that the highest percentage increase in the use of money mule accounts were for from accounts belonging to those aged between 40 and 60.[64]

54. Whilst financial firms are actively trying to prevent money mule accounts from being opened up, it is often existing and genuine accounts that are repurposed as mule accounts over time. One example of this is students who no longer need their account selling the log in details. This was reported in the Guardian:

> Students are selling their bank accounts–giving someone else their account details such as logons–for as little as £50 to £100, often as they are finishing university and heading abroad for a period. These accounts are then used by fraudsters to evade the strict checking procedures when individuals try to open an account.[65]

55. Megan Butler told us that the FCA expects banks to have "effective transaction monitoring arrangements"[66] to detect changes in account usage in order to identify changes when a mule takes over.

56. ***Financial firms who allow members of the public to open bank accounts should provide information about what a money mule is, and the penalties for being convicted, at the point of opening. This should take the form of an easy to read factsheet, rather than being buried in the small print of terms and conditions.***

57. ***Where groups of people most susceptible to being persuaded to become money mules are identified, targeted campaigns should be undertaken. For example, banks should fund work with universities, youth organisations, community centres, schools, Further Educational institutions and sixth form colleges to provide students with information, both when they join and at graduation. Targeted campaigns where other emerging trends are identified should also be undertaken.***

58. ***We recommend that the FCA should set a challenging timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently. We understand the argument made by the FCA that a timeframe***

60 Q692
61 Nationwide (ECR0089)
62 Metro Bank (ECR0092)
63 CIFAS, Fraudscape 2019, June 2019, p12
64 CIFAS, Fraudscape 2019, June 2019, p10
65 "Fraud: here's how the scammers get away with it", The Guardian, 7 July 2018
66 Q862

***may encourage financial firms to work towards the prescribed timeframe, rather than as quickly as possible, but without a deadline, some accounts are remaining open for weeks allowing further fraud to occur unnecessarily.***

## Interactions with third-party providers

59. Not all data breaches which lead to economic crime stem from failures of the banking industry. Barclays told us:

> As organisations within all sectors collect an increasing amount of consumers' data–and as the value of that data increases–the increased likelihood of data breaches will potentially leave consumers' ever-more vulnerable to fraud.[67]

60. Examples of data breaches have been covered in the press. In August 2018 a data breach at British Airways led to approximately 245,000 British Airways customers having their personal data, including payment details, stolen by hackers.[68] Similarly, in the early part of 2018, Ticketmaster was also hacked and customer's payment details also taken.[69]

61. Given such leaks of customer information, the financial sector argue that it is not able to stop economic crime alone as third-party participation in the solutions are needed. Barclays said:

> Broader and cross-sectoral collaboration is required from all organisations in the "scams ecosystem" - banks, telecommunications firms, social media platforms, dating websites, and many more-to prevent criminals from even reaching a customer in the first place.[70]

62. Which? also explained that "It is important that wherever a system's vulnerabilities are exploited, the most appropriate bodies, […] [take] responsibility and work together.[71]

63. UK Finance provided some examples of how the collaboration across the 'scams ecosystem' was already underway:

> One example of […] collaboration is the work we have undertaken with Ofcom and the telecommunications sector to help mitigate the threat of fraud and the harm it causes to consumers. […]
>
> • all UK landline service providers have implemented changes to their infrastructure, reducing the length of time a call remains connected from two minutes down to circa two seconds; […].[72]

The latter point refers to instances where a fraudster tries to prove they are from a consumers' bank by asking them to call the bank via the number on their bank card. However, the fraudster remains on the line and the consumer speaks to the same person.

67 Barclays (ECR0081)
68 "British Airways hack: why record £183m fine could have been far greater", The Week, 8 July 2019
69 "Ticketmaster sued after 2018 data breach", Ticketing Business News, 8 April 2019
70 Barclays (ECR0094)
71 Which? (ECR0044)
72 UK Finance (ECR0088)

64. UK Finance also identified many areas where work was in progress, including raising awareness of phishing, ensuring Ofcom are aware of new frauds and working to try and stop number spoofing.[73]

65. Barclays explained to us that it was often banks who ended up reimbursing consumers as a result of third party breaches, and how this could result in a lack of incentives for third parties to improve their security:

> While a data breach may be the result of insufficient cyber security and data protection procedures, it is often banks that must incur the costs of reimbursing consumers, whether it be in pre-emptive action such as the re-issuance of new cards, or in payment following the instance of a fraud or scam.
>
> We recommend that the liability framework for merchant data breaches is reviewed and updated to ensure that those who allow data losses bear the full costs of such losses, including the costs of third parties which can be accurately associated to their data loss. Otherwise, those who allow their perimeters to be breached will never have a robust incentive to protect data in the first place.[74]

66. Barclays called for data sharing across the Government and different sectors as it is critical in "preventing and halting fraud"[75] and also for the Government and regulators to use their powers under GDPR to fine firms which suffer data breaches.[76]

67. The FCA told us that the third parties in question will often be under the jurisdiction of the Information Commissioner's Office and 'subject to those regulations'.[77] Megan Butler said that the FCA works closely with the Information Commissioner's office to ensure that "regulators can work together."[78] Chris Hemsley, of the PSR, said they were engaging with "our fellow sectoral regulators–energy, water and so on–[…]to identify what more could be done."[79]

68. ***When third parties are responsible for data breaches which lead to associated fraud, they should be responsible for the associated costs. The Government should consider making third parties liable for associated costs to financial services firms and encourage the Information Commission to take this account when fining firms under the General Data Protection Regulations.***

## De-risking

69. De-risking—where a financial institution ends a customer relationship it deems to be too high risk—was a topic covered in detail in our *Economic Crime - Anti-money laundering supervision and sanctions implementation* report. The focus of that Report was

73 UK Finance (ECR0088)
74 Barclays (ECR0081)
75 Barclays (ECR0081)
76 Barclays (ECR0081)
77 Q887
78 Q887
79 Q887

the wider picture and the effect that de-risking had on economic crime and whether the practice of de-risking could lead to greater illegal activity. Here we look at how de-risking affects individuals and small businesses.

70. De-risking has been a topic of concern for us and previous Treasury Committees. Previously the Committee has heard that charities, faith-based institutions, and money transfer businesses are often the victims of de-risking. For instance, in 2016 Dr John Low of the Charities Aid Foundation told the Committee that one bank had closed 2,500 bank accounts of charities.[80] A report published in 2018 showed that 79% of charity respondents had problems accessing mainstream banking channels.[81]

71. In this inquiry, we received evidence that whole sectors, such as pawnbrokers, were having their banking services withdrawn, or refused in the first place.[82] When consumers are 'de-risked' this is often done without explanation and without giving consumers an avenue to query the decision.[83]

72. Witnesses told us de-risking could lead to "cash economies where illegal activities flourish."[84] They also warned this could increase inequality within society as much of modern society requires access to banking services.[85] The FCA Economic crime report suggested that 1.15 million customers had been refused access to financial services and around 375,000 had had their access removed.[86] Megan Butler of the FCA, went on to say that this is a "relatively small proportion of the overall number of customer transactions."[87]

73. When asked about how financial institutions approached de-risking, Megan Butler said that the FCA "expect" instances to be dealt with on a case-by-case basis, but that:

> We do come across examples, when they are brought to our attention, where it is not clear to us why an individual has been debanked;[88] we follow those up with banks when they are brought to our attention, and sometimes that leads to facilities being re-offered.[89]

74. Megan Butler went on to explain that the FCA was working on gaining more of an understanding about the prevalence and trends within the de-risking of customers:

> We will get a great deal more information coming through following the Payment Account Regulations coming into force on what the banks themselves are doing about refusal of bank accounts. […] not only will it give us a sector-wide view of trends, […] but it will give us firm-specific views on whether there are characteristics across that that would cause us concern, and […] if we see that operating.

80 Access to basic retail banking services, HC 808 Q257
81 Charity Finance Group, Impact of Money laundering and Counter-Terrorism Regulations on Charities, March 2018
82 National Pawnbrokers Association (ECR0086)
83 National Pawnbrokers Association (ECR0086)
84 The White Collar Crime Centre (ECR0026)
85 The White Collar Crime Centre (ECR0026)
86 FCA, Financial crime: analysis of firm's data, November 2018, p7, para 3.6
87 Q847
88 Debanked is a term used when someone has their bank account removed
89 Q883

> […] We will get much better data, which will allow us to tackle some of those broader societal issues in the right way and, importantly, get the banks to tackle them in the right way too.

75. Artificial Intelligence (AI) is being used to help financial firms identify financial crime.[90] As part of our *IT failures in the financial services sector inquiry*, we heard about the potential risks associated with the use of Artificial Intelligence.91 There is also evidence to suggest that AI could mirror unconscious bias from its input data92 meaning, amongst other things, it could unknowingly introduce bias against protected characteristics.[93]

76. **In the first instance banks should be as transparent as possible on de-risking to allow all individuals and firms the best possible chance of keeping their financial services. This may include providing greater information about why services have been withdrawn. There are examples of good practice on this and the FCA should ensure its rules allow for that to happen.**

77. **The FCA has at times appeared unable to act to prevent de-risking from happening. The improved data gathering from the Financial Crime Report should assist it in its efforts. *The FCA and Financial Ombudsman Service should ensure that all instances of de-risking where a customer cannot come to resolution with their bank are fully investigated and banking services returned as quickly as possible wherever possible and appropriate. We would expect to see timely and appropriate action taken where instances of blanket de-risking are apparent.***

78. ***Banks should only use Artificial Intelligence if they have a high degree of assurance that its use will not result in bias. Regulators have a role to play to ensure it is used responsibility and does not pose indiscriminate risks to sections of society.***

90 How artificial intelligence is fighting financial crime, Fintech News, 17 June 2019
91 Treasury Committee, IT failures in the financial services sector', 28 October 2019
92 Is Artificial Intelligence Racist?; Racial and Gender Bias in AI, Towards Data Science, 2 April 2019
93 As defined by the Equality Act 2010

# 3 Investigating fraud as a crime

79. The City of London Police are the national policing lead for economic crime. They also operate Action Fraud, which is the national reporting centre for fraud. Action Fraud send reports to the National Fraud Intelligence Bureau who then pass them to police forces.

80. The National Economic Crime Centre was launched in October 2018 and includes representatives from the City of London of Police, FCA and Home Office, amongst others. It is tasked with tackling economic crime in the "most efficient way."[94]

## Challenges

81. We heard a number of concerns about how law enforcement had been dealing with economic crime, and the lack of resource allocated to it.

82. Karen Baxter, the Police National Coordinator for Economic Crime, told us that in recent years the police had been operating with a reduced headcount and finances and that "fraud and economic crime has been less of a priority for policing."[95] A report published in April 2019 by Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) quoted one officer as saying "fraud does not bang, bleed, or shout"[96] as an explanation as to why it is not always a high priority for police forces.

83. The Police are not the only body who undertake investigations of financial crime. Where the police are unable to investigate a fraud, other bodies may take up the investigation. Andrew Bailey, Chief Executive Officer at the FCA told us:

> One of the issues that we are also facing here, […] is the lack of capacity in the broader system for tackling fraud. […] We tackle this stuff but we are not a fraud investigator per se. We are having to do a lot more of it.[97]

84. Peter O'Doherty, Head of Crime and Cyber at the City of London Police described the challenges faced by the police, and others when investigating economic crime:

> I would say that a significant number, if not the majority, of economic crime cases are enabled by changing technology. In some cases, we are looking for a ghost. We are looking for a machine, a botnet or a DDoS [Distributed Denial of Service attack] that has committed this offence. It is how you recruit the right people into policing, with the right skills, how you keep them and how you make sure that we can match the pace at which criminals develop these capabilities. It always feels like we are behind and that is really difficult. One of the reasons why some of the cases are not investigated, whether it is a high loss or a low loss, is because the only line of inquiry we have is a website in a jurisdiction that we cannot touch or it is a piece of technology we just do not know how to get round.[98]

94 National Economic Crime, Improving the UK's response to economic crime, accessed 15 October 2019
95 Q565
96 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p5
97 Treasury Committee, Oral evidence: Independent Review of the Financial Ombudsman Service, HC1400, 22 January 2019, Q499
98 Q594

## Fraud strategy

85. The City of London Police is the lead for economic crime nationwide and is responsible for prevention and investigation.[99] Karen Baxter, the Police National Coordinator for Economic Crime, told us that "[T]he benefits of having a national lead force and central co-ordination is that we understand where those trends can start to emerge."[100] However the HMICFRS report appeared to question whether there was a central lead for the investigation of economic crime. It stated that:

> There is no national strategy for tackling fraud. […] Police forces have therefore developed a range of different responses. We found some examples of good practice but, taken as a whole and given the scale of fraud, not enough is being done. When it exists, good practice is not always disseminated or widely adopted.[101]

86. As a result of its criticism of the lack of a central fraud strategy, the HMICFRS recommended that the National Economic Crime Centre (NECC) should be involved in setting a national strategy. The HMICFRS report explained that the NECC is:

> A multi-agency centre [that] is expected to improve the understanding of the serious and organised economic crime threat, and plan and co-ordinate the response to the most harmful cases.[102]

87. Karen Baxter of the City of London Police told the Committee that the NECC "is a really good step that brings all of the assets across law enforcement together and extends that further into partnership with finance and with banking."[103]

88. The Government's *Economic Crime Plan 2019–22*, published during the course of this inquiry, does set a national strategy for combatting economic crime. It proposes to utilise the NECC and one of the Plan's commitments is to "[C]ontinue to develop the NECC as a genuine public-private hub for combatting serious and organised economic crime."[104] The Plan also includes actions to be implemented by the NECC alongside other bodies which include improving the policing response to fraud,[105] improving education around economic crime threats[106] and improving information sharing.[107]

89. **The announcement of a national fraud strategy is long overdue. It followed the damning criticism of Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services' report. It must now be a priority for police forces to make the strategy work. *One of the actions from the Economic Crime Plan 2019–22 is that the police response to fraud is improved. The Government should provide us with an update on this action within six-months of publication of this report.***

99 City of London Police, Advice and support, accessed June 2019
100 Q572
101 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p7
102 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p17
103 Q565
104 HM Government, Economic Crime Plan 2019–22, July 2019, p19, point 20
105 HM Government, Economic Crime Plan 2019–22, July 2019, p39, point 5.7
106 HM Government, Economic Crime Plan 2019–22 July 2019, p48, point 6.8
107 HM Government, Economic Crime Plan 2019–22, July 2019, p62, Action 46

## Investigating complex fraud

90. Particularly complex frauds stretch the resources of individual police forces. As the HMICFRS report noted:

> From time to time, particularly serious, large-scale frauds, often involving organised crime groups, will come to light. When such cases are not taken on by the Serious Fraud Office, it will fall to the police (or the National Crime Agency) to investigate them, or they may decide not to. We recognise that such cases can involve difficult decisions and the long-term commitment of significant resources.[108]

91. An example of such a case was the prosecution of the so-called HBOS Reading Fraud. This fraud involved bank staff and consultants defrauding small business owners. Following the conclusion of that case, which is currently subject to independent review, total compensation offers of more than £96m have been made to victims.[109] Anthony Stansfeld, Police and Crime Commissioner, Thames Valley, noted that in that case:

> 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. Neither the Serious Fraud Office nor Financial Conduct Authority (FCA) has the capacity to take on major banking fraud.[110]

92. When we asked Karen Baxter, the Police National Coordinator for Economic Crime, how large and complex frauds should be investigated, she accepted that there had been problems in the past:

> You are quite right that there were cases in the past that had moved around various organisations. The whole establishment of the National Economic Crime Centre is designed to design that out, if at all possible. There will always be a clash of agendas and cultures across organisations. What I would like to reassure the panel of is that I see less of that today. I see absolutely less of that today than I saw 15 years ago, and that is really a good, positive thing. I see an absolutely collective will to have discussions, to have multilateral work and to have bilateral work.[111]

Karen Baxter also provided context as to why cases may be moved around:

> There is also a concern, if I am being very frank. Every force has a finite amount of resources, people and money. UK policing has a dearth of detectives. We are absent in the numbers we would like. Therefore, every force, every ROCU [Regional Organised Crime Unit] and the City of London feels that. When there is a case that comes to a particular police force, there is naturally sense of, "Is it ours or who does it belong to?" In terms of a case meeting a certain threshold, if it comes to the City of London, it will have a

108 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, para 5.73

109 Lloyds Banking Group, Lloyds Banking Group announces the conclusion of HBOS Reading customer review by Professor Griggs, 7 May 2019

110 Police and Crime Commissioner Thames Valley, Statement from the Police and Crime Commissioner - Fraud, 19 January 2018

111 Q596

> threshold whereby we would test whether it needs to be investigated by the City of London. Equally, if it goes to a ROCU or if it goes to the National Economic Crime Centre, is it set in absolute stone that it is ABC?.[112]

93. The HMICFRS report described weaknesses in how the 'tasking' of cases (referring cases upward) worked:

> We found no formal process to request City of London Police, as the national lead force for fraud, to take on an investigation. National and regional tasking processes were generally not used for fraud so that individual forces became responsible for major cases that involved cross-border or national criminality. We were told of large-scale frauds 'bouncing around' between agencies with no agency taking responsibility for them.[113]

To deal with this, the HMICFRS recommended that:

> With immediate effect, the Director General of the National Crime Agency, in consultation with the National Police Chiefs' Council Coordinator for Economic Crime, should ensure that the tasking powers of the National Crime Agency are used effectively in the case of serious and organised fraud.[114]

94. Karen Baxter also emphasised that following the HBOS Reading case:

> What I can give you an assurance of is that it is something that is very much to the fore of how we are working as the national lead force with colleagues across ROCUs [Regional Organised Crime Units]. There are a number of pilots that we are working with at the moment to try to pull out how we would task or how we would allocate those particular cases, and, equally as importantly, how, when those cases go out to a force and start to be investigated and it starts to become known that it is a much bigger case, we escalate those through efficiently and in a timely manner to where it needs to go. I cannot give you what I think you are looking for but I can give you the reassurance that it is absolutely at the forefront of our minds to deal with that.[115]

95. However, she also told us she was " not entirely aware of" another significant and well publicised case, the so called 'tuna bonds' alleged $2 billion fraud, this lack of awareness perhaps itself a demonstration of the pressures on police resources.

96. **Complex fraud cases have not always been effectively 'tasked' or referred upwards. At times they are just moved from pillar to post. This is unacceptable for the victims of potentially devastating crimes. It is therefore welcome that this is both a focus of the police, and its inspectorate.**

112 Q597
113 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p17
114 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p75
115 Q598

97. **Improvements to tasking will hopefully relieve some pressure on local forces. However, some cases will remain at the local level. *The Government must review how it provides support to individual police forces which consider they have complex frauds they could successfully investigate, where resources may otherwise prevent those cases progressing.***

## Reporting

98. Action Fraud is designed to monitor the landscape of economic crime. Karen Baxter, the Police National Coordinator for Economic Crime, explained to the Committee why Action Fraud is important:

> The benefit of having that central reporting system, which is very much the envy of other countries and other law enforcement, is that, while it is not perfect, it allows us to start to mine and bring all of that data together. It allows us to use the intelligence and to understand the offending types.[116]

99. In addition to Action Fraud, there is also a voluntary role for financial firms to play in alerting the police when they note trends or potential crimes in action. Karen Baxter said that financial firms were mainly "sharing information at the appropriate time and at the earliest opportunity",[117] but she also said this was not happening in every case, especially where the financial firm had reimbursed the consumer and did not deem the loss worth the "bureaucracy that it would take to inform [the police]."[118] When asked if this information would be useful, Karen Baxter told us "Would I like them to contact us? Yes, I would. Would I like that information and intelligence? Yes, I would. Could we use that going forward? Absolutely."[119]

100. **We are pleased to hear that in the main, reports of economic crime from financial institutions to the police are happening in a timely manner so the police can start an investigation promptly. However, we are concerned that banks do not always appear to be reporting instances to the police where, for example, the bank has reimbursed the victim. Given the high-speed nature of the financial system, any delay in reporting to the police could prevent recovery of funds and allow fraudsters to profit at a victim's expense. *The Government should require all frauds to be reported regardless of their size, and whether or not a financial institution has reimbursed a consumer.***

## Action Fraud

101. We also heard evidence, that consumers were often unclear about how to report an economic crime, and/or about what Action Fraud could achieve. Richard Piggin, Head of External Affairs, Which?, told us:

> Action Fraud does not have investigative powers. They collate that, which is useful to get a sense of the general trends of fraud. They might pass it on to the NFIB [National Fraud Intelligence Bureau], which might pass it back to a local police force, if there is a case for it to be investigated. Now, this takes

116 Q574
117 Q576
118 Q577
119 Q577

> time. It often comes back to the local police force and you will get a letter to say, "There is no viable lead of inquiry, so your case is closed." In general, it is a very unsatisfactory experience.[120]

102. Action Fraud has recently been the subject of media investigations which focused on the working practices of staff[121] and what happens to information provided to Action Fraud.[122] These reports suggested that significant improvements were needed by Action Fraud to ensure staff consistently treat victims with sympathy and were being clear to victims as to how the information will be used. Yvette Cooper, Chair of the Home Affairs Committee said that "Action Fraud has become a means to divert and fob off victims of crime."[123]

103. Concerns were also raised about Action Fraud in the HMICFRS report. Amongst them, it noted that:

> The 2006 Fraud Review stated that it was confusing for victims to know where to report fraud and recommended that a national fraud reporting centre should be established. Thirteen years later, confusion still exists. The Office for National Statistics identified in 2018 that the main reason for not reporting fraud was "a lack of awareness of Action Fraud".[124]

The HMICFRS report also raised concerns about how calls were being handled:

> The average call abandonment rate for Action Fraud for the 12 months to March 2018 was 37 percent. This was an increase on the previous year's figure of 34 percent. Average call waiting time in March 2018 was 16 minutes, having increased over the previous two years.[125]

104. Given its concerns, the HMICFRS report, recommended that:

> By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should provide guidance to Action Fraud and chief constables. This is to ensure that, promptly on reporting a fraud, victims are provided with explanations of:
>
> - the role of Action Fraud;
> - the process by which their fraud report will be considered for assessment or referral to the police (or other law enforcement agency) by the National Fraud Intelligence Bureau; how to obtain an update on the progress of their case;
> - how, following referral from the National Fraud Intelligence Bureau, the decision on whether and how to investigate rests with the police (or other law enforcement agency); and

120 Q544
121 The Times, Action Fraud investigation: victims misled and mocked as police fail to investigate, published 15 August 2019
122 Which? Magazine, Why the system is failing scam victims, October 2019
123 The Times, Action Fraud investigation: victims misled and mocked as police fail to investigate, published 15 August 2019
124 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p18
125 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p18

- the options open to victims of fraud to seek civil redress as an alternative (in cases where criminal investigations are not carried out or do not lead to convictions).[126]

105. **It is not currently always clear to consumers whether a fraud should be reported to an individual consumer's bank, the police or to Action Fraud, nor is it always clear what each entity would do with the information provided. The process for reporting an economic crime needs to be clarified. We welcome the plans to issue guidance to Action Fraud and chief constables to ensure consumers reporting a crime are clearly told both how reported instances of fraud will be used, and also how they won't be used, when they report a crime.**

106. **The serious criticism of Action Fraud in the 'Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services' report and in the media need to be addressed. In its response to this report the Government should set out what it has done to address this issue.**

126 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, Fraud: Time to Choose, April 2019, p25

# 4 Consumer rights and responsibilities

107. Consumers have always faced economic crime and fraudsters attempting to part them from their money. However, as we have seen, while economic crime is not new, the methods for committing frauds themselves are becoming increasing sophisticated, requiring fresh thinking on consumer protection. Susan Allen of Santander UK told us:

> As the scammers and fraudsters become more sophisticated, it is quite right that we evolve our understanding of what is right and fair for customers to do to protect themselves.[127]

In this chapter we consider the balance between consumers' rights and responsibilities, including reimbursement, gross negligence and education.

## Contingent Reimbursement Model

108. As part of its efforts to tackle the growing rise of APP fraud, in April 2018 the Payment Systems Regulator (PSR) set up a steering group to set up a voluntary industry code to show when victims of APP Fraud should be reimbursed. This followed a super-complaint by Which? to the PSR in September 2016. The group produced the Contingent Reimbursement Model (CRM) Code, which came into effect on 28 May 2019.

109. The Code covers payments made via CHAPS, Faster Payments and internal book transfers.[128] The Code set outs the circumstances under which the financial firms who have signed the Code should reimburse the money lost; the types of information financial firms should provide consumers so they can make informed decisions; and the responsibilities financial firms have if they are sending or receiving payments.[129]

110. On 1 July 2019 the Lending Standards Board (LSB) took over responsibility for the governance and oversight of the Code. Ruth Evans, the Independent Chair of the Authorised Push Payments Scams Steering Group, told us that the LSB entered into a memorandum of understanding with the Steering Group which included specifying the mechanisms by which the code would be reviewed, both thematically and as a whole.[130] She also confirmed that there would be a review within the first year, and subsequently rolling reviews every three years.[131]

111. The Code is a voluntary undertaking by relevant financial firms. When we asked why a voluntary code had been chosen, rather than making changes to legislation or regulation, Ruth Evans of the Authorised Push Payments Scams Steering Group told the Committee that the "PSR felt this was the best way forward" and that the voluntary nature meant that changes could be made more quickly:

127 Q640
128 APP Scams Steering Group, Draft Contingent Reimbursement Model Code, September 2018, para 3.13
129 Lending Standards Board, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 28 May 2019
130 Q808
131 Q813

> It could be done and introduced far more swiftly, and more responsively to consumer and industry needs. […] Introducing a voluntary code […], in essentially a year, is much faster than any statutory underpinning, which would require legislation.[132]

112. The Code has been welcomed by banks. Barclays, for example, told us that the Code marked "a major improvement in consumers' protection against the impact of scams."[133] However, Richard Piggin of Which? cautioned that the success [of the Code] would be judged on the impact it had on consumers.[134]

113. The LSB has a list of all financial firms who have currently signed up to the Code on its website.[135] Despite this not being all firms which offer banking facilities, Chris Hemsley of the PSR told us that he believes the principles put into the Code would become "industry best practice" and that the Financial Ombudsman Service would see the them as "standards that [would] need to be applied in any event."[136]

114. **We welcome the Contingent Reimbursement Model Code—a frame work for financial institutions to use to determine when reimbursement should be provided to victims of APP Fraud—as a way to protect consumers.** ***We remain unpersuaded that the Code should be voluntary and strongly urge any relevant parties who have not yet signed up to the Code to do so. As the first year review of the Code approaches, the Code should now be made compulsory through legislation.***

### *Retrospective reimbursement*

115. While the introduction of the Contingent Reimbursement Model Code will cover future victims of fraud if their financial provider was a signatory to the Code, it does not provide any resolution to previous victims of such frauds. Victims and those who represent them told us they believed the Code should also be applied retrospectively.[137] The reasons they gave included that it would be unjust to exclude victims prior to the Code's implementation and the fact there are no legislative or regulatory changes which have led to the Code's development.[138]

116. As part of its consultation into the development of a Code, the PSR received evidence from individuals in favour of retrospective reimbursement, but also received submissions from financial services providers who disagreed with retrospection because the standards of the model could not be retroactively implemented.[139] No explanations as to why it could not be retroactively implemented were provided in the consultation publication.

132 Q812
133 Barclays (ECR0081)
134 Q534
135 Lending Standards Board, Contingent Reimbursement Model Code (CRM) for Authorised Push Payment Scams, October 2019
136 Q879
137 Holly Richardson (ECR0084), Barrie Cooper (ECR0079) and 4Keys International (ECR0076)
138 Holly Richardson (ECR0084)
139 Payment Systems Regulator, Authorised push payment scams: Reponses to our consultation on the development of a contingent reimbursement model, February 2018

117. When asked why the original parameters of the Code set by the PSR did not cover retrospective reimbursement, Ruth Evans, Independent Chair of the Authorised Push Payments Scams Steering Group, told us that it was recognised that "Payment service providers [could not] retrospectively implement or adhere to the standards of the model."[140] The PSR explained that:

> Applying the Code's standards retrospectively means payment service providers (PSPs) would have to compensate customers based on standards that didn't exist at the time of the fraud. Given the Code's voluntary nature, this would have been a major barrier to getting PSPs to sign up, meaning customers would most likely not be enjoying the protections they have now.[141]

That said, the PSR did not restrict any financial entity from continuing to "be able to offer goodwill payments"[142] in retrospective circumstances

118. **We accept that including retrospective reimbursement within the Code would have been a barrier to financial firms becoming signatories. However, financial firms have been warned since 2016, when Which? made a super complaint, that they have been failing in their duty to protect customers by not linking information on account names to payments. This is still an issue as Confirmation of Payee has not been implemented yet.**

119. ***We strongly encourage firms to consider whether refusing to retrospectively reimburse customers who relied on the payee name is fair and just. We especially encourage this where the customer would now fall into the Code's definition of vulnerability.***

## Practitioner Guide

120. In order to ensure the Code is properly implemented, a Practitioner Guide for those financial institutions that sign up to the Code has been produced. Ruth Evans of the Authorised Push Payments Scams Steering Group told the Committee that content of the guide was being "overseen by both a consumer and a PSP, with input from everybody from the steering group as well."[143]

121. Richard Lloyd, who was an Advisor to the Authorised Push Payments Scams Steering Group explained the function of the Practitioner Guide to the Committee:

> The practitioner guide gives a very clear set of examples of what kinds of activity the banks should be undertaking and what view they should take of different consumer approaches to the level of care. […] The practitioner guide is intended to give people on the frontline a clear sense of what is expected of them across the industry, what good looks like and what is unacceptable.[144]

140 Payment Systems Regulator, Report and Consultation, Authorised push payment scams, November 2017, p45, para 6.49
141 Payment Systems Regulator (ECR0096)
142 Payment Systems Regulator, Report and Consultation, Authorised push payment scams, November 2017, p45, para 6.49
143 Q805
144 Q807

122. In addition to the Practitioners Guide there is a guide for consumers. This guide gives a high-level overview of the types of scams a consumer may face, general warnings as to what to look out for when making a payment, and what to do if a consumer falls victim to a scam.[145] The Consumer Guide and the Practitioner Guide, as described by Richard Lloyd, appear to differ in that the Consumer Guide provides no specific examples.

123. Richard Lloyd told the Committee that the Practitioner Guide would not be made available to consumers as the steering group "obviously do not want it to become a guide for fraudsters."[146]

124. **We accept that keeping the Practitioner Guide private avoids it becoming a guide to committing fraud. However, the current consumer guidance is so high level, it does not give consumers a clear sense of what is expected of them. Without sight of how the Code should work in practice, consumers may be left unable to effectively challenge their bank. This could lead to an increased number of cases being referred to the Financial Ombudsman Service and a delay in any potential reimbursement. We recommend that a more detailed consumers' guide is produced, which includes practical examples.**

## Recovery of stolen funds

125. Until January 2019, consumers who were the victim of authorised or unauthorised fraud could only claim against their own financial services provider, and not the provider that received the funds. The FCA have issued new rules, which came into force on 31 January 2019, permitting consumers to complain to the financial firm receiving the payment. These firms now have the same obligations as the firm sending the payment under the complaints handling procedures within the FCA Handbook.[147] Megan Butler of the FCA told us that:

> Victims now have a greater capacity to go to the FOS [Financial Ombudsman Service] to complain if their bank has not stepped up to the mark, or indeed if the payee bank has not stepped up to the standards that they are expected to meet.[148]

126. Until recently, financial firms have only had access to information within their own firms. As such they could not see how payments moved across the entire banking system. The Mule Insights Tactical Solution (MITS), run by Vocalink, brings together data across the banking system to analyse transactions and see how laundered funds are moved.[149] Mark Tingey of Metro Bank told us that the technology "is helping to proactively identify prospective mules based on activity from other accounts."[150] The technology is used to track suspicious payments "regardless of whether the payment amount is split between multiple accounts, or those accounts belong to the same or different financial institutions."[151]

145 Lending Standards Board, Authorised Push Payment Scam – Information for Customers on the Voluntary Code, May 2019
146 Q807
147 FCA, FCA introduces new rules on handling complaints about Authorised Push Payment fraud, December 2018
148 Q846
149 Faster Payments, New anti-money laundering technology sees UK fraud rings frozen, December 2018
150 Q749
151 Faster Payments, New anti-money laundering technology sees UK fraud rings frozen, December 2018

127. Despite the existence of the MITS, it is still usually not possible for payments to be recovered when the receiving account has been identified. This is because recovery and payment of the funds out of the recipient account can currently only take place with direct authority of the account holder.[152] Susan Allen of Santander UK, explained:

> We are tracking where payments go. Even when we find that money has gone to an account, today you cannot get it back. Unless you have the authority of the account holder to remove that money, you cannot remove that money even if you have suspicion.[153]

The receiving bank is only liable if they have neglected their responsibilities as set out in FCA Handbook.

128. Stephen Jones, Chief Executive of UK Finance, also highlighted the frustrations with the current legal framework:

> Fundamentally, when we are talking about victims, if we can identify where the victim's money has gone but cannot do anything about repatriating the money from the end account to the victim, something is wrong in the system. Unfortunately it is the law that prevents that at the moment.[154]

129. **We welcome the FCA's recent rule changes requiring financial firms receiving payments to ensure that they are not inadvertently assisting economic crime. However, we are concerned by the lack of power financial institutions have to recover money sitting in bank accounts once it has been reported as stolen.** ***Given the development of MITS technology, the Government should review the current legislation around recovery of stolen funds to ensure that victims can be reimbursed as quickly as possible, whilst protecting legitimate transactions.***

## Gross negligence

130. Where a firm concludes that a loss from an unauthorised fraud was down to the consumer's own 'gross negligence', reimbursement is unlikely. The Payment Services Regulations 2017[155] state that the consumer would be liable for all losses on an unauthorised payment if (amongst other criteria) they are deemed to be grossly negligent. Gross negligence can include not using the payment instrument (for example a debit or credit card) in the agreed manner with the service provider.[156]

131. Whilst regulations use the concept of 'gross negligence', they did not provide a definition. Stephen Jones of UK Finance told the Committee this meant that:

> The interpretation of gross negligence, to the extent that there is no statutory definition, becomes a matter of common law. When the FOS [Financial Ombudsman Service] look at the concept of gross negligence, they apply a judgment every time in terms of what they think is fair and reasonable. It is a matter of interpretation and practice.[157]

152 Q663
153 Q663
154 Q663
155 The Payment Services Regulations 2017, No.752, Part 7, Section 77(3)(b)
156 The Payment Services Regulations 2017, No.752, Part 7, Section 72(1)(a)
157 Q679

132. This ambiguity in determining what amounted to gross negligence was echoed by Mark Tingey of Metro Bank, who told us that 'Unfortunately, there is no definition and very little case law in terms of gross negligence.'[158]

133. It is therefore down to individual financial firms to decide what constitutes 'gross negligence'. The Financial Ombudsman notes that there is "an ever-changing state of play"[159] with regards to the scams being faced by consumers. Firms may differ, therefore, in deciding what are "fair and reasonable"[160] expectations for consumers. One solution could be for cases to be referred to the FOS, but under the current arrangements this would be at a consumers' discretion, and it might take time for an accepted view to develop of what gross negligence meant in a certain case.

134. Caroline Wayman, Chief Ombudsman and Chief Executive of the FOS, stated that their policy was to set "gross negligence [at] a pretty high bar."[161] Examples the Committee were given by industry representatives for what might be considered to be negligent included giving someone the PIN for a bank card, or not storing the PIN safely;[162] and not ensuring the loss of a bank card is reported promptly.[163]

135. Despite the existence of the term 'gross negligence' in the regulatory framework, we were told that firms were reluctant to use it when corresponding with customers to avoid upsetting the customer.[164] Susan Allen of Santander UK told the Committee "We have never automatically called a customer grossly negligent."[165] Mark Tingey of Metro Bank told us that its process was not to use the phrase as they felt explaining the rationale of the decision was more helpful than using the phrase.[166]

136. However, Richard Emery, an independent fraud investigator, argued that as the rules state a consumer is only liable for all losses if they have been 'grossly negligent', unless the bank proves and states this, they should be reimbursing.[167]

137. We were told that firms would take the vulnerability of a customer into account when determining whether a customer had acted negligently. During our inquiry into Consumer Access to Financial Services we were told about how Eleanor Southwood, Chair of the Royal National Institute of Blind People, needed to give her PIN to a taxi driver because the Chip and PIN device was not able to cater to those with partial sighting.[168] When asked on this specific case, Chris Rhodes, of Nationwide, said "We have a vulnerability policy, and cases are assessed on a case-by-case basis. […] which we would always take into account."[169]

158 Q726
159 Financial Ombudsman Service, Ombudsman News - fraud and scams: a moving picture, August 2018
160 Financial Ombudsman Service, Ombudsman News - fraud and scams: a moving picture, August 2018
161 Treasury Committee, Oral evidence: Independent Review of the Financial Ombudsman Service, HC1400, 22 January 2019, Q225
162 Q671
163 Q684
164 Q530
165 Q641
166 Q731–732
167 Q543
168 Treasury Committee, Oral evidence: Consumers' access to financial services, HC1642, 14 November 2018, Q89
169 Q673

138. Vulnerability is not dependent on the protected characteristics listed in the Equality Act 2010.[170] In our report *Consumer' access to financial services* we took evidence on the FCA definition of vulnerability and how it could be applied in practice. As part of their response to our report, the FCA promised a consultation on 'Guidance for firms on the fair treatment of vulnerable customers' which was launched in July 2019.[171] This consultation has now closed and we are awaiting the results. The consultation noted that vulnerability may stem from circumstances, for example bereavement, and as such a consumer could be vulnerable for a period of time, and not their whole life.[172]

139. **The existing Payment Services Regulations do not define what actions by a customer would be deemed as 'gross negligence'. As a result, each individual firm can set its own bar of what customer behaviour it would deem to be grossly negligent. This could lead to a lack of consistency between how customers with the same circumstances are treated.** ***We recommend that an accepted definition for gross negligence should be agreed by the regulators. The regulators should require financial firms to produce an easy to read lists of 'dos and don'ts' for customers, to show how the individual financial firms would define proper account usage in the majority of circumstances. Such lists would allow for variations between firms.***

140. **Financial firms must ensure that vulnerability is a key factor in determining if a consumer was grossly negligent.** ***The FCA should ensure that the outputs from their recent consultation on the Guidance for Firms on the Fair Treatment of Vulnerable Customers covers any finding of gross negligence.***

141. ***If firms do find individual consumers to have been grossly negligent, we recommend their customer responses quote the legislation the firms are relying upon to refuse making a reimbursement, alongside an explanation of how this conclusion was reached. Although it may cause distress, we believe that using the phrase 'grossly negligent' would provide a very clear explanation to the consumer why their claim is being refused, and on what grounds.***

## Public education

142. Despite the scale of economic crime, Detective Chief Superintendent Peter O'Doherty, Head of Crime and Cyber at the City of London Police, told us that the general public are largely unaware of economic crime unless they themselves have been a victim:

> Cybercrime and economic crime is a big problem once you have been victimised but, up until that point, for an average person, it is a fairly invisible crime.[173]

170 Equality Act 2010
171 FCA, Guidance for firms on the fair treatment of vulnerable customers, July 2019
172 FCA, Guidance for firms on the fair treatment of vulnerable customers, July 2019, para 2.3
173 Q572

143. During our inquiry we gathered evidence on how best to educate consumers both on general advice around how to avoid being the victim of a scam, and on ensuring they were aware of specific scams. We heard evidence about the various educational pieces that regulators,[174] trade bodies,[175] the police[176] and individual banks[177] have undertaken.

144. We heard differing opinions on how effective the education push by the financial sector has been. Mark Tingey of Metro Bank said that "people are more aware today of the threats that are out there than they maybe were five years ago."[178] However Richard Piggin of Which? was more sceptical about whether increased education had lead to any reduction in fraud:

> [The banks] response to date has focused very much on education and awareness-raising, […] and we are not convinced that there is enough evidence to show that education and awareness-raising has an impact on reducing the amount of fraud.[179]

145. TSB provided evidence to us describing outreach sessions in areas where data was showing a higher likelihood of falling victim to fraud. As a result of these sessions the attendees reported "that they felt more confident in being able to spot fraud after attending."[180]

146. Education must reach as many consumers as possible in accessible ways in order to be effective. Mark Steward, Executive Director of Enforcement and Market Oversight at the FCA, explained to us that while a lot of education campaigns may seem to be "basic" information, it was important for messages to be repeated to people for it to be fully understood:

> People often forget about [financial education] when they are being induced to make an investment by someone who turns out to be a fraudster or a scamster […]That kind of information needs to be repeated over and over again to really get it through to people, so that they understand that they are at risk of being scammed.[181]

147. An example of such an education piece was the "Take Five" campaign run by the Home Office and Joint Fraud Taskforce partners on a national basis. This utilised different types of media to send a simple message to consumers around how to protect themselves from fraud. Karen Baxter the Police National Coordinator for Economic Crime, explained the key message within the campaign:

> If it looks too good and feels too good, it is probably too good. It is about the power of getting people to take five minutes and to take a step back. That in itself will have prevented many crimes.[182]

174 Q902
175 Q693
176 Q595
177 Q692, Q748
178 Q725
179 Q523
180 TSB (ECR0093)
181 Q902
182 Q596

148. **Education has an important role to play in the wider fight against economic crime. There is always merit in equipping consumers with skills to give them the confidence and knowledge to pause and think about whether or not the situation they have found themselves in could be a fraud.**

149. ***We recommend that financial firms should undertake targeted education campaigns where trends have been identified and when new scams appear. These should include information at the point of opening an account about the consequences of being a money mule and information regarding emerging frauds so that consumers can stay vigilant.***

150. ***It is important that financial education is not a 'one time' exercise. We recommend that reminders are sent out to consumers in different formats and at different times. This should include online marketing and social media to target messages to younger consumers. This will ensure that firms are not only meeting their obligations of the Contingent Reimbursement Model Code, but also will help prevent fraudsters from succeeding in the first place.***

# Conclusions and recommendations

## The type and scale of economic crime affecting consumers

1. It is clear, both in terms of financial losses and in the variety of scams suffered by consumers, that economic crime is a serious and growing problem in the UK. Trends need to be identified quickly. *In order to ensure a clear picture of the scale and types of economic crime facing consumers, the FCA should publish data on economic crime within six months. It should evolve its data collection practices to ensure they allow for emerging trends, while still enabling year-on-year comparisons.* (Paragraph 15)

## Prevention

2. The Government has not been listening to concerns that data sharing requirements for financial services firms are too restrictive and unfit for purpose. *We welcome the establishment of the public-private working group. Its remit must include assessing whether the current data sharing requirements are fit for purpose. If not, the working group must make detailed proposals to reform those legal requirements including considering using existing subordinate legislation-making powers under the Data Protection Act 2018 to amplify or clarify exemptions in the Act. The group should report to us every six months on progress made.* (Paragraph 24)

3. We are concerned over the length of time some accounts used in economic crime remain active once intelligence has been received on their potential misuse. Whilst we understand that prescribed timeframes could delay how quickly banks act, the difference in time each bank takes to act creates weakness in the UK financial system. *The FCA should work with financial institutions to ensure consistency across the sector. We recommend that the FCA uses its powers to set a timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently.* (Paragraph 28)

4. Confirmation of payee will not solve economic crime alone, and as such the onus will always be on financial firms to develop further methods and technologies to keep up with fraudsters. (Paragraph 39)

5. The fact that banks were not previously confirming payees is a serious failure to protect customers from harm. Asking for such information but not using it would have created a false sense of security among some customers when sending payments. It might have been better for banks to not ask for this information at all if they were not going to use it for fraud prevention. (Paragraph 40)

6. *We therefore recommend that Confirmation of Payee should be introduced as a matter of urgency. Every delay leaves more people vulnerable to falling victim to economic crime. If the implementation date of March 2020 begins to look in doubt, regulators should consider introducing sanctions, such as fines, to firms who have not met the deadline.* (Paragraph 41)

7. The arguments put forward that Confirmation of Payee implementation could be harmful for competition if large firms implemented before small ones, is without

merit. Competition in the banking sector exists for the benefit of customers, not for the benefit of firms. Customers should not be put at risk of becoming victims of fraud, in order to protect slow adopting firms from implementing protections for their customers. *The Payment Systems Regulator should therefore ensure that all relevant firms can implement Confirmation of Payee by the end of 2020.* (Paragraph 42)

8. Subtle differences which might not be immediately obvious to many people, such as using 'soliciters' rather than 'solicitors', could represent a fruitful way for fraudsters to disguise fraudulent accounts as legitimate accounts, and therefore small inaccuracies should be flagged for consumers' own protection. *We recommend that spelling mistakes are flagged within the new Confirmation of Payee System.* (Paragraph 43)

9. Fraudsters rely on the speed of the payment system to move money into a series of different accounts before a customer or a customer's bank are aware that a fraud has taken place. The speed of transactions make it difficult for banks to trace stolen money once a fraud has occurred. Very few first-time payments need to be received instantaneously. Very large payments will often be scheduled days in advance. Therefore, high-speed payments on first time payments could be made redundant with only a limited impact on consumers. (Paragraph 49)

10. *We recommend a mandatory 24-hour delay on all initial or first-time payments, during which time a consumer about to be defrauded could remove themselves from the high-pressure environment in which they are being manipulated. All future payments to that same account could flow at normal speed to minimise inconvenience to customers. If a situation arose whereby an initial payment was needed instantly, a customer could ring their bank and additional checks could be carried out for the funds to be released.* (Paragraph 50)

11. Financial firms who allow members of the public to open bank accounts should provide information about what a money mule is, and the penalties for being convicted, at the point of opening. This should take the form of an easy to read factsheet, rather than being buried in the small print of terms and conditions. (Paragraph 56)

12. Where groups of people most susceptible to being persuaded to become money mules are identified, targeted campaigns should be undertaken. For example, banks should fund work with universities, youth organisations, community centres, schools, Further Educational institutions and sixth form colleges to provide students with information, both when they join and at graduation. Targeted campaigns where other emerging trends are identified should also be undertaken. (Paragraph 57)

13. *We recommend that the FCA should set a challenging timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently. We understand the argument made by the FCA that a timeframe may encourage financial firms to work towards the prescribed timeframe, rather than as quickly as possible, but without a deadline, some accounts are remaining open for weeks allowing further fraud to occur unnecessarily. (Paragraph 58)*

14. *When third parties are responsible for data breaches which lead to associated fraud, they should be responsible for the associated costs. The Government should*

*consider making third parties liable for associated costs to financial services firms and encourage the Information Commission to take this account when fining firms under the General Data Protection Regulations.* (Paragraph 68)

15. In the first instance banks should be as transparent as possible on de-risking to allow all individuals and firms the best possible chance of keeping their financial services. This may include providing greater information about why services have been withdrawn. There are examples of good practice on this and the FCA should ensure its rules allow for that to happen. (Paragraph 76)

16. The FCA has at times appeared unable to act to prevent de-risking from happening. The improved data gathering from the Financial Crime Report should assist it in its efforts *The FCA and Financial Ombudsman Service should ensure that all instances of de-risking where a customer cannot come to resolution with their bank are fully investigated and banking services returned as quickly as possible wherever possible and appropriate. We would expect to see timely and appropriate action taken where instances of blanket de-risking are apparent.* (Paragraph 77)

17. *Banks should only use Artificial Intelligence if they have a high degree of assurance that its use will not result in bias. Regulators have a role to play to ensure it is used responsibility and does not pose indiscriminate risks to sections of society.* (Paragraph 78)

## Investigating fraud as crime

18. The announcement of a national fraud strategy is long overdue. It followed the damning criticism of Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services' report. It must now be a priority for police forces to make the strategy work. *One of the actions from the Economic Crime Plan 2019–22 is that the police response to fraud is improved. The Government should provide us with an update on this action within six-months of publication of this report.* (Paragraph 89)

19. One of the actions from the Economic Crime Plan 2019–22 is that the police response to fraud is improved. The Government should provide us with an update on this action within six-months of publication of this report. (Paragraph 89)

20. Complex fraud cases have not always been effectively 'tasked' or referred upwards. At times they are just moved from pillar to post. This is unacceptable for the victims of potentially devastating crimes. It is therefore welcome that this is both a focus of the police, and its inspectorate. (Paragraph 96)

21. Improvements to tasking will hopefully relieve some pressure on local forces. However, some cases will remain at the local level. *The Government must review how it provides support to individual police forces which consider they have complex frauds they could successfully investigate, where resources may otherwise prevent those cases progressing.* (Paragraph 97)

22. We are pleased to hear that in the main, reports of economic crime from financial institutions to the police are happening in a timely manner so the police can start an investigation promptly. However, we are concerned that banks do not always appear to be reporting instances to the police where, for example, the bank has

reimbursed the victim. Given the high-speed nature of the financial system, any delay in reporting to the police could prevent recovery of funds and allow fraudsters to profit at a victim's expense. (Paragraph 100)

23. The Government should require all frauds to be reported regardless of their size, and whether or not a financial institution has reimbursed a consumer. (Paragraph 100)

24. It is not currently always clear to consumers whether a fraud should be reported to an individual consumer's bank, the police or to Action Fraud, nor is it always clear what each entity would do with the information provided. The process for reporting an economic crime needs to be clarified. We welcome the plans to issue guidance to Action Fraud and chief constables to ensure consumers reporting a crime are clearly told both how reported instances of fraud will be used, and also how they won't be used, when they report a crime. (Paragraph 105)

25. The serious criticism of Action Fraud in the 'Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services' report and in the media need to be addressed. In its response to this report the Government should set out what it has done to address this issue. (Paragraph 106)

## Consumer rights and responsibilities

26. We welcome the Contingent Reimbursement Model Code—a frame work for financial institutions to use to determine when reimbursement should be provided to victims of APP Fraud—as a way to protect consumers *We remain unpersuaded that the Code should be voluntary and strongly urge any relevant parties who have not yet signed up to the Code to do so. As the first year review of the Code approaches, the Code should now be made compulsory through legislation.* (Paragraph 114)

27. We accept that including retrospective reimbursement within the Code would have been a barrier to financial firms becoming signatories. However, financial firms have been warned since 2016, when Which? made a super complaint, that they have been failing in their duty to protect customers by not linking information on account names to payments. This is still an issue as Confirmation of Payee has not been implemented yet. (Paragraph 118)

28. *We strongly encourage firms to consider whether refusing to retrospectively reimburse customers who relied on the payee name is fair and just. We especially encourage this where the customer would now fall into the Code's definition of vulnerability.* (Paragraph 119)

29. We accept that keeping the Practitioner Guide private avoids it becoming a guide to committing fraud. However, the current consumer guidance is so high level, it does not give consumers a clear sense of what is expected of them. Without sight of how the Code should work in practice, consumers may be left unable to effectively challenge their bank. This could lead to an increased number of cases being referred to the Financial Ombudsman Service and a delay in any potential reimbursement. We recommend that a more detailed consumers' guide is produced, which includes practical examples. (Paragraph 124)

30. We welcome the FCA's recent rule changes requiring financial firms receiving payments to ensure that they are not inadvertently assisting economic crime. However, we are concerned by the lack of power financial institutions have to recover money sitting in bank accounts once it has been reported as stolen. *Given the development of MITS technology, the Government should review the current legislation around recovery of stolen funds to ensure that victims can be reimbursed as quickly as possible, whilst protecting legitimate transactions.* (Paragraph 129)

31. The existing Payment Services Regulations do not define what actions by a customer would be deemed as 'gross negligence'. As a result, each individual firm can set its own bar of what customer behaviour it would deem to be grossly negligent. This could lead to a lack of consistency between how customers with the same circumstances are treated. *We recommend that an accepted definition for gross negligence should be agreed by the regulators. The regulators should require financial firms to produce an easy to read lists of 'dos and don'ts' for customers, to show how the individual financial firms would define proper account usage in the majority of circumstances. Such lists would allow for variations between firms.* (Paragraph 139)

32. Financial firms must ensure that vulnerability is a key factor in determining if a consumer was grossly negligent. *The FCA should ensure that the outputs from their recent consultation on the Guidance for Firms on the Fair Treatment of Vulnerable Customers covers any finding of gross negligence.* (Paragraph 140)

33. *If firms do find individual consumers to have been grossly negligent, we recommend their customer responses quote the legislation the firms are relying upon to refuse making a reimbursement, alongside an explanation of how this conclusion was reached. Although it may cause distress, we believe that using the phrase 'grossly negligent' would provide a very clear explanation to the consumer why their claim is being refused, and on what grounds.* (Paragraph 141)

34. Education has an important role to play in the wider fight against economic crime. There is always merit in equipping consumers with skills to give them the confidence and knowledge to pause and think about whether or not the situation they have found themselves in could be a fraud. (Paragraph 148)

35. *We recommend that financial firms should undertake targeted education campaigns where trends have been identified and when new scams appear. These should include information at the point of opening an account about the consequences of being a money mule and information regarding emerging frauds so that consumers can stay vigilant.* (Paragraph 149)

36. *It is important that financial education is not a 'one time' exercise. We recommend that reminders are sent out to consumers in different formats and at different times. This should include online marketing and social media to target messages to younger consumers. This will ensure that firms are not only meeting their obligations of the Contingent Reimbursement Model Code, but also will help prevent fraudsters from succeeding in the first place.* (Paragraph 150)

# Formal minutes

## Tuesday 22 October 2019

Members present:

Catherine McKinnell took the Chair, in accordance with the Resolution of the Committee of 9 September

Rushanara Ali Alison McGovern

Alison Thewliss

Draft Report (*Economic Crime: Consumer View*), proposed by the Chair, brought up and read.

*Ordered*, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 150 read and agreed to.

Summary agreed to.

*Resolved*, That the Report be the Third Report of the Committee to the House.

*Ordered*, That the Chair make the Report to the House.

*Ordered*, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 29 October at 9.15 a.m.

# Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

### Tuesday 15 May 2018

**Duncan Hames**, Director of Policy, Transparency International UK, **Naomi Hirst**, Senior Campaigner, Global Witness, **Tom Keatinge**, Director, Centre for Financial Crime and Security Studies, Royal United Services Institute — Q1–72

### Tuesday 19 June 2018

**Stephen Curtis**, Chairman, The Association of Company Registration Agents (ACRA), **Adam Harper**, Director of Strategy & Professional Standards, AAT, **Mark Hayward**, Chief Executive, NAEA Propertymark — Q73–172

### Wednesday 4 July 2018

**Donald Toon**, Prosperity Command, National Crime Agency, **Mark Thompso**n, Interim Director, Serious Fraud Office — Q173–262

### Tuesday 9 October 2018

**Colin Bell**, Group Head of Financial Crime Risk, HSBC, **Stephen Jones**, CEO, UK Finance — Q263–339

### Wednesday 10 October 2018

**Rena Lalgie**, Director, Office of Financial Sanctions Implementation, HM Treasury, **Simon York**, Director, Fraud Investigation Service, HM Revenue and Customs, **Alison Barker**, Director of Specialist Supervision, Financial Conduct Authority — Q340–426

### Tuesday 30 October 2018

**John Glen MP**, Economic Secretary to the Treasury, **Rt Hon Ben Wallace MP**, Minister of State for Security at the Home Office, **Robert Buckland QC MP**, Solicitor General — Q427–513

### Tuesday 27 November 2018

**Richard Piggin**, Head of External Affairs, Which, **Richard Emery**, Independent Fraud Investigator, 4Keys International — Q514–563

## Tuesday 8 January 2019

**Police Commander Karen Baxter**, Police National Coordinator for Economic Crime, City of London Police, **Detective Chief Superintendent Peter O'Doherty**, Head of Crime and Cyber, City of London Police — Q564–622

## Wednesday 13 February 2019

**Stephen Jones**, Chief Executive, UK Finance, **Susan Allen**, Head of Retail Business Banking, Santander UK, **Chris Rhodes**, Chief Product and Propositions Officer, Nationwide Building Society — Q623–721

## Tuesday 2 April 2019

**Mark Tingey**, Head of Financial Crime Operations, Metro Bank — Q722–789

**Ruth Evans**, Independent Chair, Authorised Push Payments Scams Steering Group, Richard Lloyd, Advisor, Authorised Push Payments Scams Steering Group — Q790–836

## Wednesday 15 May 2019

**Megan Butler**, Executive Director, Investment, Wholesale and Specialists Division, **Chris Hemsley**, Co-Managing Director, Payment Systems Regulator, **Mark Steward**, Executive Director of Enforcement and Market Oversight, FCA — Q837–915

# Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

ECR numbers are generated by the evidence processing system and so may not be complete.

1 4Keys International (ECR0076)

2 4keys International (ii) (ECR0077)

3 ABI (ECR0052)

4 ACRA (ECR0069)

5 Additional written evidence from the Office of Financial Sanctions Implementation (ECR0072)

6 APP Scams Steering Group (ECR0095)

7 Association of Accounting Technicians (AAT) (ECR0012)

8 Association of Certified Fraud Examiners (ECR0003)

9 The Association of Company Registration Agents (ACRA) (ECR0013)

10 The Bar of Northern Ireland (ECR0030)

11 Barclays (ECR0081)

12 Barclays (ECR0094)

13 Bond Anti-Corruption Group (ECR0036)

14 Bournemouth University (ECR0045)

15 Campaign for Fairer Gambling (ECR0021)

16 Campbell, Professor Liz (ECR0009)

17 Centre for Economic Performance / London School of Economics (ECR0040)

18 The Chartered Institute of Taxation (CIOT) (ECR0011)

19 Cifas (ECR0037)

20 City of London Police (ECR0057)

21 City of London Police (ECR0090)

22 Cooper, Barrie (ECR0079)

23 CORE Coalition (ECR0029)

24 Corruption Watch (ECR0028)

25 Deutsche Bank UK, Financial Crime Investigations (ECR0053)

26 Emery, Richard (ECR0083)

27 FCA (ECR0010)

28 Financial Conduct Authority (ECR0071)

29 Fraud Advisory Panel (ECR0034)

30 Global Witness (ECR0027)

31 Heathershaw, Dr John (ECR0017)

32 HM Revenue and Customs (ECR0070)

33 HM Treasury (ECR0097)

34 Home Office (ECR0078)
35 HSBC (ECR0063)
36 Hurford, Mr David (ECR0001)
37 ICAEW (ECR0024)
38 JH Dragon Network (ECR0049)
39 Keep Me Posted (ECR0043)
40 The Law Society (ECR0041)
41 Levi, Professor Michael (ECR0023)
42 LexisNexis Risk Solutions (ECR0005)
43 Lyddon Consulting (ECR0091)
44 Master Card Vocalink (ECR0085)
45 Mather & Co Solicitors (ECR0058)
46 Metro Bank (ECR0092)
47 MIDAS Alliance (ECR0032)
48 Money Saving Expert (ECR0062)
49 NAB Customer Support Group (ECR0054)
50 NAEA Propertymark (ECR0039)
51 National Crime Agency (ECR0073)
52 National Pawnbrokers Association (ECR0086)
53 National Trading Standards (ECR0016)
54 Nationwide (ECR0089)
55 Office for National Statistics (ECR0082)
56 Payment Systems Regulator (ECR0015)
57 Payment Systems Regulator (ECR0096)
58 Petrol Retailers and Car Wash Associations (ECR0055)
59 Post Office (ECR0042)
60 R3 (ECR0066)
61 Richardson, Holly (ECR0084)
62 RICS (ECR0059)
63 Rights and Accountability in Development (RAID) (ECR0035)
64 RUSI Centre for Financial Crime and Security Studies (ECR0018)
65 Ryder, Dr Nicholas (ECR0031)
66 Santander (ECR0080)
67 Santander (ECR0087)
68 Serious Fraud Office (ECR0038)
69 Serious Fraud Office (supplementary) (ECR0068)
70 Solicitors Regulation Authority (ECR0014)
71 Standard Chartered Bank (ECR0050)

72 STEP (ECR0022)

73 Thinking about Crime Limited (ECR0002)

74 Thomas, Simon (ECR0025)

75 Thomson Reuters (ECR0051)

76 Transparency International UK (ECR0004)

77 TSB (ECR0093)

78 UK Finance (ECR0064)

79 UK Finance (ECR0088)

80 UK Finance (ii) (ECR0065)

81 UK Finance (iii) (ECR0074)

82 UK Finance (iv) (ECR0075)

83 University of Sheffield Management School (ECR0033)

84 Visa Europe (ECR0061)

85 Which? (ECR0044)

86 The White Collar Crime Centre (ECR0026)

87 Yoti (ECR0048)

# List of reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

## Session 2019–20

| | | |
|---|---|---|
| First Report | Impact of Business Rates on Business | HC 222 |
| Second Report | IT Failures in the Financial Services Sector | HC 224 |
| First Special Report | The work of the Financial Conduct Authority: the perimeter of regulation: FCA response to the Committee's Thirty-Fifth Report of Session 2017–19 | HC 132 |

## Session 2017–19

| | | |
|---|---|---|
| First Report | Appointment of Sir Dave Ramsden as Deputy Governor for Markets and Banking at the Bank of England | HC 472 |
| Second Report | Appointment of Professor Silvana Tenreyro to the Bank of England Monetary Policy Committee | HC 471 |
| Third Report | The Solvency II Directive and its impact on the UK Insurance Industry | HC 324 (HC 863) |
| Fourth Report | Transitional arrangements for exiting the European Union | HC 473 (HC 850) |
| Fifth Report | Autumn Budget 2017 | HC 600 (HC 757) |
| Sixth Report | Appointment of Elisabeth Stheeman to the Financial Policy Committee | HC 758 |
| Seventh Report | Student Loans | HC 478 (HC 995) |
| Eighth Report | Appointment of Charles Randell as Chair of the Financial Conduct Authority and the Payment Systems Regulator | HC 838 |
| Ninth Report | Childcare | HC 757 (HC 1196) |
| Tenth Report | Re-appointment of Alex Brazier to the Financial Policy Committee | HC 936 |
| Eleventh Report | Re-appointment of Donald Kohn to the Financial Policy Committee | HC 937 |
| Twelfth Report | Re-appointment of Martin Taylor to the Financial Policy Committee | HC 938 |
| Thirteenth Report | The Motability Scheme | HC 847 |

| | | |
|---|---|---|
| Fourteenth Report | Re-appointment for Gertjan Vlieghe to the Monetary Policy Committee | HC 1056 |
| Fifteenth Report | Women in finance | HC 477<br>(HC 1567) |
| Sixteenth Report | Appointment of Bradley Fried as Chair of Court, Bank of England | HC 1319 |
| Seventeenth Report | Appointment of Professor Jonathan Haskel to the Monetary Policy Committee | HC 1318 |
| Eighteenth Report | Appointment of Andy King to the Budget Responsibility Committee of the OBR | HC 1340 |
| Nineteenth Report | Household finances: income, saving and debt | HC 565<br>(HC 1627) |
| Twentieth Report | Appointment of Jill May to the Prudential Regulation Committee | HC 1511 |
| Twenty-first Report | Appointment of Professor Julia Black to the Prudential Regulation Committee | HC 1512 |
| Twenty-second Report | Crypto-assets | HC 910<br>(HC 1845) |
| Twenty-third Report | Re-appointment of Sir Jon Cunliffe as Deputy Governor for Financial Stability at the Bank of England | HC 1626 |
| Twenty-fourth Report | SME Finance | HC 1626<br>(HC 1873) |
| Twenty-fifth Report | The UK's economic relationship with the European Union: The Government's and Bank of England's Withdrawal Agreement analyses | HC 805 |
| Twenty-sixth Report | Budget 2018 | HC 1819 |
| Twenty-seventh Report | Appointment of Kathryn Cearns as Chair of the Office of Tax Simplifications | HC 1606<br>(HC 2111) |
| Twenty-eighth Report | Economic Crime - Anti-money laundering supervision and sanctions implementation | HC 2012 |
| Twenty-ninth Report | Consumers' access to financial services | HC 2010<br>(HC 2187)<br>(HC 2530<br>(HC 2535) |
| Thirtieth Report | Re-appointment of Michael Saunders to the Monetary Policy Committee | HC 1642<br>(HC 2423) |
| Thirty-first Report | Re-appointment of Dr Ben Broadbent as Deputy Governor for Monetary Policy at the Bank of England | HC 2294 |
| Thirty-second Report | The appointment of Dame Colette Bowe to the Financial Policy Committee | HC 2235 |
| Thirty-third Report | The re-appointment of Professor Anil Kashyap to the Financial Policy Committee | HC 2237 |
| Thirty-fourth Report | Disputing tax | HC 1914 |
| Thirty-fifth Report | The work of the Financial Conduct Authority: the perimeter of regulation | HC 2594 |

| | | |
|---|---|---|
| First Special Report | Transitional arrangements for exiting the European Union: Government Response to the Treasury Committee's Fourth Report | HC 850 |
| Second Special Report | The Solvency II Directive and its impact on the UK Insurance Industry: Bank of England Response to the Committee's Third Report of session 2017–19 | HC 863 |
| Third Special Report | Autumn Budget 2017: Government and Office for Budget Responsibility responses to the Treasury Committee's Fifth Report | HC 757 |
| Fourth Special Report | Student Loans: Government and Office for National Statistics responses to the Committee's Seventh Report | HC 995 |
| Fifth Special Report | Childcare: Government Response to the Committee's Ninth Report | HC 1196 |
| Sixth Special Report | Women in finance: Government Response to the Committee's Fifteenth Report | HC 1567 |
| Seventh Special Report | Household finances: income, saving and debt: Government Response to the Committee's Nineteenth Report | HC 1627 |
| Eighth Special Report | Government and Financial Conduct Authority Responses to the Committee's Twenty-Second Report: Crypto-assets | HC 1627 |
| Ninth Special Report | Government and Financial Conduct Authority Responses to the Committee's Twenty-Fourth Report: SME Finance | HC 1873 |
| Tenth Special Report | Government Response to the Twenty-Sixth Report: Budget 2018 | HC 2111 |
| Eleventh Special Report | Government Response to the Committee's Twenty-Eighth Report: Economic Crime - Anti-money laundering supervision and sanctions implementation | HC 2187 |
| Twelfth Special Report | Consumers' Access to Financial Services: Financial Conduct Authority response to the Committee's Twenty-Ninth Report | HC 2423 |
| Thirteenth Special Report | Consumers' Access to Financial Services: Government Response to the Committee's Twenty-Ninth Report | HC 2530 |
| Fourteenth Special Report | Consumers' Access to Financial Services: Payment Systems Regulator and Bank of England responses to the Committee's Twenty-Ninth Report | HC 2535 |
| Fifteenth Special Report | The work of the Financial Conduct Authority: the perimeter of regulation: Government Response to the Committee's Thirty-fifth Repor | HC 2674 |