House of Commons

Committee of Public Accounts

The growing threat of online fraud

Sixth Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 27 November 2017

HC 399
Published on 6 December 2017
by authority of the House of Commons

The Committee of Public Accounts

The Committee of Public Accounts is appointed by the House of Commons to examine "the accounts showing the appropriation of the sums granted by Parliament to meet the public expenditure, and of such other accounts laid before Parliament as the committee may think fit" (Standing Order No. 148).

Current membership

Meg Hillier MP (*Labour (Co-op), Hackney South and Shoreditch*) (Chair)

Bim Afolami MP (*Conservative, Hitchin and Harpenden*)

Heidi Allen MP (*Conservative, South Cambridgeshire*)

Geoffrey Clifton-Brown MP (*Conservative, The Cotswolds*)

Martyn Day MP (*Scottish National Party, Linlithgow and East Falkirk*)

Chris Evans MP (*Labour (Co-op), Islwyn*)

Caroline Flint MP (*Labour, Don Valley*)

Luke Graham MP (*Conservative, Ochil and South Perthshire*)

Andrew Jones MP (*Conservative, Harrogate and Knaresborough*)

Gillian Keegan MP (*Conservative, Chichester*)

Shabana Mahmood MP (*Labour, Birmingham, Ladywood*)

Nigel Mills MP (*Conservative, Amber Valley*)

Layla Moran MP (*Liberal Democrat, Oxford West and Abingdon*)

Stephen Morgan MP (*Labour, Portsmouth South*)

Bridget Phillipson MP (*Labour, Houghton and Sunderland South*)

Gareth Snell MP (*Labour (Co-op), Stoke-on-Trent Central*)

Powers

Powers of the Committee of Public Accounts are set out in House of Commons Standing Orders, principally in SO No. 148. These are available on the Internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website 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 Richard Cooke (Clerk), Dominic Stockbridge (Second Clerk), Hannah Wentworth (Chair Support), Ruby Radley (Senior Committee Assistant), Kutumya Kibedi (Committee Assistant), and Tim Bowden (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Committee of Public Accounts, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6593; the Committee's email address is pubaccom@parliament.uk.

Contents

Summary

Online fraud is now the most prevalent crime in England and Wales, impacting victims not only financially but also causing untold distress to those affected. The cost of the crime is estimated at £10 billion, with around 2 million cyber-related fraud incidents last year, however the true extent of the problem remains unknown. Only around 20% of fraud is actually reported to police, with the emotional impact of the crime leaving many victims reluctant to come forward. The crime is indiscriminate, is growing rapidly and shows no signs of slowing down. Urgent action from government is needed, yet the Home Office's response has been too slow and the banks are unwilling to share information about the extent of fraud with customers. The balance needs to be tipped in favour of the customer. Online fraud is now too vast a problem for the Home Office to solve on its own, and it must work with a long list of other organisations including banks and retailers, however it remains the only body that can provide strategic national leadership. Setting up the Joint Fraud Task in 2016 was a positive step, but there is much still to do. The Department and its partners on the Joint Fraud Taskforce need to set clear objectives for what they plan to do, and by when, and need to be more transparent about their activities including putting information on the Home Office's website.

The response from local police to fraud is inconsistent across England and Wales. The police must prioritise online fraud alongside efforts to tackle other sorts of crime. But it is vital that local forces get all the support they need to do this, including on identifying, developing and sharing good practice.

Banks are not doing enough to tackle online fraud and their response has not been proportionate to the scale of the problem. Banks need to take more responsibility and work together to tackle this problem head on. Banks now need to work on information sharing so that customers are offered more protection from scams. Campaigns to educate people and keep them safe online have so far been ineffective, supported by insufficient funds and resources. The Department must also ensure that banks are committed to developing more effective ways of tackling card not present fraud and that they are held to account for this and for returning money to customers who have been the victims of scams.

Introduction

The growth of the internet and advances in digital technologies have created great opportunities for innovation and economic growth, but also more opportunities for online crime. Online criminals can target thousands of victims at the same time, causing financial and emotional harm to people and harm to businesses' finances and reputations. In the year to September 2016 there were an estimated 1.9 million incidents of cyber-related fraud in England and Wales. The true cost of online fraud is unknown, but is likely to be billions of pounds a year. The Home Office (the Department) is responsible for preventing and reducing crime, including online fraud. Many other bodies also play a role, including the police, banks and Action Fraud (which is run by the City of London Police). In 2016 the Department set up the Joint Fraud Taskforce to improve collaboration between all bodies in tackling online fraud.

Conclusions and recommendations

1. **Banks do not accept enough responsibility for preventing and reducing online fraud and there is no data available to assess how well individual banks are performing.** Banks have an important role to play in protecting customers but the protection they provide is variable and some are keener to invest in educating customers and anti-fraud technology than others. Banks can refuse to reimburse customers who have been scammed and 'voluntarily' transferred money, and shifting more responsibility onto banks for scams is likely to make them better at protecting customers. Banks are not required to provide complete data on their individual performances to the government or police, and no-one knows which banks are best at protecting them from fraud. The banks argued that data on individual banks performance would help fraudsters target the weakest banks. We can see that full detail in the public domain about which banks are more susceptible to what kinds of fraud could prove counter-productive, but there is clearly scope for more transparency over individual banks' performance at a more aggregated level. Customers have the right to know at least something about individual banks' record on protecting customers from fraud. Besides more transparency from the banks, there is also scope for more help from banks for vulnerable people, such as putting restrictions on their bank accounts so they are not at risk of losing huge amounts of money.

   Recommendation: ***The Department should set out minimum standards for banks to follow on preventing online fraud and on protecting bank customers and require banks to report to government on their performance. The Department should press the banking industry to make relative online fraud vulnerability performance data publicly available. We expect the Department to provide us with a plan for publication of this data by Spring 2018. We encourage banks to develop a voluntary scheme in the meantime to be more open with customers about the extent of fraud and how they are tackling it.***

2. **Unless all banks start working together, including making better use of technology, there will be little progress on tackling card fraud and returning money to customers.** Card not present fraud, where criminals use stolen card details, has been rising dramatically in recent years. The 1.4 million known incidents in 2016 was double the number from 5 years earlier. Technical innovations to tackle card not present fraud will only be successful if every bank participates, as they did for Chip and PIN, but solutions are still some way off. The Department wants to see a 'significant reduction' in card not present fraud but says it is not yet in a position to quantify what that means. People also transfer funds themselves to fraudsters, unaware until later that they are the victims of scams. Somewhere between 40% and 70% never get their money back, and banks have different policies for under what circumstances to refund money. Banks are also reported to be holding at least £130 million that has been frozen because it is fraud related, but which cannot be accurately traced and returned to victims, often because it has been passed through numerous 'mule' accounts. The Department is taking forward an initiative with the banks to make the best use of technology to spot mule accounts and repatriate money quickly, but says it will be a couple of years before it is likely to have a fully fledged system.

Recommendation: ***Working with Joint Fraud Taskforce partners, the Department should make sure all banks to make better use of technology and information to reduce card fraud and return money to customers. This should include establishing minimum technical standards for strong customer authentication for electronic payments***

3. **We are not convinced that current awareness campaigns such as Take Five are proving effective.** Many people are still not aware of how to keep safe online, and the government and others run numerous ongoing campaigns to improve citizens' and businesses' cyber security. While there is a perception that online fraud primarily affects the elderly and vulnerable, young people are increasingly likely to fall victim. Social media plays a significant role in online scams and further education is needed to make young people aware of the dangers of sharing personal information online. The City of London Police told us that young people are probably more vulnerable to fraud than older generations as they have a very different approach to personal information. The City of London Police cited examples of young people sharing pictures of their passports and driving licences on social media. The government should consider this in its running and targeting of campaigns to maximise impact. The Take Five Campaign backed by the government was re-launched in October 2017 with total funding of £3.8 million, £500,000 of which is from the government. A lack of co-ordination and consistency in education campaigns can confuse the public and reduce campaigns' impact. There is often low awareness of campaigns, which are often not tailored for specific groups, and which can also confuse the public and reduce impact. Age UK highlighted huge scope to do more on education to support victims and help prevent them becoming victims again. The Department is evaluating Take Five but the evaluation is not due to be completed until March 2018.

   Recommendation: ***The Department, working with others on the Joint Fraud Taskforce, needs to develop a more informed approach to its education campaigns—being specific about what it is trying to achieve, evaluating what works best, and looking at opportunities for campaigns more targeted at specific groups.***

4. **The Department has not yet put in place effective arrangements for its oversight of a coordinated and effective response to online fraud and for reporting on its progress.** The Department is not solely responsible for reducing and preventing online fraud, but is in overall charge and is the only body that can provide the necessary strategic leadership. Many other bodies also play a role, including the police, banks, and Action Fraud, the national reporting centre for fraud. The Department is only now making fraud a priority, most notably launching the Joint Fraud Taskforce in February 2016, although fraud is not a new problem and the government's work in this area for over 10 years appears not to have led anywhere. The Department itself considers there is an "enormous amount to be done", but relies on voluntary participation from industry and law enforcement in the Taskforce. While reassuring us about its 'scale of ambition', the Department has no sense yet of how to quantify what success would look like, not even a range for what might be plausible to achieve. On the day before our evidence session the Department finally made some information about the Taskforce's work publicly available on its website for the first time.

Recommendation: ***The Department should develop specific plans for how it will measure progress in tackling online fraud and judge the success of the Joint Fraud Taskforce, and it should regularly publish information on progress and performance. It should update us on progress by the end of March 2018.***

5. **The Department lacks data to judge whether its response to tackling online fraud is working.** Effective action can only be underpinned properly if the Department understand the nature and scale of the threat. Yet the Department only first started to attempt to measure fraud in 2016 and when it did found that fraud accounted for a third of all crime—3.6 million fraud incidents, of which the majority was online fraud. In the same period around 623,000 incidents were actually recorded, just 20% of estimated online fraud. The main reasons fraud is not reported to the police are because people are too embarrassed, report their loss to the bank and do not take it further, have difficulties in making a report, or simply do not report it because they think nothing will happen. The day after our evidence session plans to launch a new hotline for victims of fraud were reported in the press, but no such plans had been mentioned to us. The City of London Police highlighted how important it is to share information to prevent crime, but there is no formal requirement for banks to report fraud or share reports with government or the police. The City of London Police is introducing a new Action Fraud system to make it easier for people to report fraud and to collect information to help government and others understand the threat better. The police would also like to have a "harm index" for online fraud so it could measure whether the action being taken is actually reducing harm against the public.

   Recommendation: ***The Department must prioritise efforts to improve the collection and reporting of data on fraud. It should update us on progress by the end of March 2018, when we also expect to hear how it is improving information sharing between government, industry and law enforcement, and working with Action Fraud to reduce the gap between reported and actual fraud.***

6. **The response to tackling online fraud is variable across different police forces, and for some it is not a priority.** Online fraud now features in a number of national strategies, and there is an expectation for local police forces to respond to national priorities, but only 27 out of 41 Police and Crime Commissioners referred to online fraud in their police and crime plans. Age UK told us that the police response to online fraud was extremely patchy and elderly people can suffer real harm and stop using their computers, unplug their phones and, in the worst cases, end up in care homes because they have been victims. Age UK said that there was a problem of local good practice being shared nationally. The Commissioner of City of London Police cannot mandate what other police forces should do, but to improve the local police response his force shares information on the level of fraud in each area; carries out peer reviews; and provides advice, best practice guidance and training. Online fraud is a high volume crime and must fit alongside everything else the police are dealing with, but this makes sharing good practice all the more important.

   Recommendation: ***The Department should, with the City of London Police, establish what more they can do to help all police forces tackle online fraud, including opportunities to identify, develop and share good practice in a more systematic way.***

1 The response from government and law enforcement

1. On the basis of a report by the Comptroller and Auditor General, we took evidence from the Home Office (the Department) and the City of London Police on the government's response to tackling online fraud. The City of London is the national policing lead for fraud and also has responsibility for Action Fraud.[1] We also took evidence from Age UK, UK Finance, Lloyds and the British Retail Consortium.

2. The growth of the internet and advances in digital technologies have created great opportunities for innovation and economic growth, but also more opportunities for online crime. While traditional crimes such as vehicle offences and house burglary have declined substantially in recent years, fraud, more than half of which is committed online, is becoming more common and is a growing threat. Online criminals can target thousands of victims at the same time, causing harm to citizens financially and emotionally and to businesses' finances and reputations. The true cost of online fraud is unknown, but is likely to be billions of pounds, with one estimate that individuals lost around £10 billion and the private sector around £144 billion in 2016.[2] However, while estimates can be made on the financial cost of online fraud, the emotional impact on victims is much more difficult to assess.

3. The Office for National Statistics estimates that there were around 1.9 million incidents of cyber-related fraud in England and Wales in the year ending 30 September 2016, or 16% of all estimated crime incidents. Online fraud includes criminals accessing citizens' and businesses' bank accounts, using their plastic card details, or tricking them into transferring money.[3]

Oversight of the response to online fraud

4. The Home Office (the Department) has overall responsibility for preventing and reducing crime, including online fraud. Many other bodies also play a role, including the police, banks, the National Fraud Intelligence Bureau which records fraud offences and shares information with police forces, and Action Fraud, the national reporting centre for fraud. In 2016 the Department set up the Joint Fraud Taskforce to improve collaboration between government, industry and law enforcement in tackling online fraud. In the same year the government published its National Cyber Security Strategy to 2021, which includes its plans for tackling cyber crime, including cyber-enabled fraud and data theft.[4]

5. With the large number of organisations that have a role in tackling online fraud, the Department described its role as "providing strategic national leadership for the country in responding to this challenge". It stressed that it could not do everything itself but has a critical role in making sure there is a strategy that is prioritised and adapted over time.[5] We drew to the Department's attention that the need to tackle online fraud is not just a very recent issue; for example, with the National Hi-Tech Crime Unit having been established

1 C&AG's Report, Online fraud, Session 2017–19, HC 45, 30 June 2017
2 C&AG's Report, paras 1–2
3 C&AG's Report, para 3
4 C&AG's Report, para 4
5 Qq 66–68

in 2001 before later being merged into the Serious Organised Crime Agency. Yet the problems reported by the National Audit Office 16 years later, such as a lack of joined-up thinking across government, communications and sharing of good practice seem to be fairly basic issues. The Department commented that, as a growing area, causing financial and emotional harm and damaging confidence in our economic system, it was taking the issue very seriously. The Department also acknowledged that there is still "an enormous amount to be done".[6]

6. Commenting on the Joint Fraud Taskforce, Lloyds (a member of the Taskforce) told us that, while it was relatively young organisation and had achieved good things, it was now time for the Taskforce to have more formality, with some specific targets and measurements. UK Finance, which represents the banking and finance industry in the UK, commented that having long-term strategic goals for the Taskforce would be useful.[7] The British Retail Consortium, which has recently joined the Taskforce, agreed. Age UK called for public commitments to action, to which people could be held accountable.[8] Age UK also commented more generally that it would like to see much more Government prioritisation of online fraud with, for example, where fraud is particularly targeted at vulnerable groups, account being taken of the impact on the victim, not just the amount of money.[9] The Department told us that it accepted the need to put more "formality and structure" around the Taskforce, and that it was doing that.[10]

7. Despite setting up the Taskforce in February 2016, the Department has not yet reported on the Taskforce's progress or established measures for its performance. The Department has not set any formal targets for what degree of reduction in fraud over what period it would consider to represent success. The Department acknowledged that the point of having a baseline measure against which to measure progress is indeed to measure progress, and wanted to reassure us about its 'scale of ambition'.[11] But the Department declined to offer us even a range of improvement for what success might look like. The Permanent Secretary commented that "we are not yet in a position of putting a figure on what success looks like" and that "Before I even gave a range, I would want to do more reflection on, and some analysis of, what will actually be plausible, and under what conditions".[12]

8. On the day before our evidence session the website for the Joint Fraud Taskforce was updated to include minutes of meetings of the oversight board as well as further information. Some of the documents were removed a few hours later. Previously the website had contained minimal information. The Department could not explain the reasons for this at the time of our session.[13] The Department did agree that "it is very important that the public know what is going on".[14] The Department acknowledged that it could have done more to share information earlier and undertook in future to share

6 Qq 69–71
7 Correspondence with UK Finance, 24 November 2017
8 Q 54
9 Q 43
10 Q 127
11 Qq 126, 127; C&AG's Report, para 12
12 Q 131, 135
13 Qq 58, 63
14 Q 59

what information it could about the Joint Fraud Taskforce much more promptly.[15] In subsequent correspondence the Home Secretary reiterated her commitment to ensuring public transparency of this activity.[16]

The collection and reporting of data on fraud

9. In the year to September 2016 the Office for National Statistics (ONS) reported an estimated 11.8 million incidents of crime in England and Wales. For the first time, the official figures revealed an estimated 3.6 million fraud incidents, of which 1.9 million (53%) were cyber-related. In the same period there were, however, only around 623,000 fraud offences actually recorded, suggesting that around 80% of incidents are not reported to the police.[17]

10. The City of London Police told us there were three main reasons why fraud is under-reported and that it is seeking to address: people feeling embarrassed about having been duped and being seen as foolish; people reporting the loss to the bank and often not also reporting it to the police; and challenges relating to the efficiency of the reporting process.[18] Age UK also told us that "At the moment, people are reluctant to report fraud because they don't think anything is going to happen".[19]

11. We highlighted our own experiences from constituents of how it can be very difficult to report an incident of fraud. For example, being told by local police that they could not take a report, and that the report should be made to Action Fraud, but then it being too difficult to get through and speak to anyone at Action Fraud. The City of London Police told us that such a response from the local police was not correct and also that there would soon be a new system that will "enable a much more fluid, user-friendly approach".[20]

12. On 19 October 2017, the day after our oral evidence session, it was reported in the press that government was considering having a new hotline specifically for victims of bank fraud and similar scams—a '555 hotline'. We were surprised that the possible new hotline had not been mentioned to us the day before. In correspondence after our session the Home Secretary clarified that the hotline had been a proposal from the financial sector at a September Joint Fraud Taskforce Oversight Board meeting, and the idea was being explored. But the Department had done no further work on it and so had not been in a position to discuss it at out evidence session.[21]

13. The City of London Police highlighted that much of the relevant data on online fraud is held by the private sector, rather than by law enforcement agencies, which is why the work being done by the Joint Fraud Taskforce to encourage data and intelligence sharing is so important.[22] However, we also note that there is no formal requirement for banks to report fraud or share reports with government. Action Fraud and the NFIB are introducing

15 Qq 61, 62, 65
16 Correspondence with Home Secretary, 1 November 2017
17 Q 58; C&AG's Report, para 6
18 Q 72
19 Q 49
20 Qq 73, 102
21 Correspondence with Home Secretary, 1 November 2017
22 Q 72

an enhanced system for collecting and analysing data to help the government and others understand the threat, but success will depend on whether the data reported to Action Fraud are comprehensive, accurate and timely.[23]

14. The Department said it hoped that the statistics published so far by the ONS, while not perfect and with some omissions, would provide it with a good baseline from which to tell in future years whether online fraud is going up, going down, or staying constant.[24] The City of London Police stressed the importance of being able to show that the crime survey for England and Wales was a good independent assessment of the level of crime, and how part of demonstrating success would be showing the gap narrowing between what is reported in the survey and what is reported to police. The police would also like to have an assessment of the harm caused to online fraud victims so it can measure whether the action being taken is actually reducing harm against the public—"That would be a great thing for us to do, to have something like a national harm index".[25]

The variable response across different police forces

15. Online fraud now features in a number of national strategies, including the 2016 Modern Crime Prevention Strategy and the National Cyber Security Strategy. There is an expectation for local police forces to respond to national priorities, but only 27 out of 41 Police and Crime Commissioners referred to online fraud in their police and crime plans as at April 2017.[26] The City of London Police told us that while relatively few forces had fraud as a priority, 41 out of 43 forces had vulnerability and protecting vulnerable victims as a priority, though that would include different crime types.[27]

16. Age UK told us that it finds the level of response to be "extremely patchy" across different geographical areas. It has known cases where victims have stopped using their computer, unplugged their phone and, in the worst case, ended up in a care home earlier than they needed to.[28] On the standard of response from the police and Action Fraud, Age UK added that the issue was not necessarily with the City of London Police, but with pushing out good practice nationally. The British Retail Consortium also noted that there are some examples of really good practice, mentioning Operation Falcon in the Met, involving dedicated and trained officers, but suspected that such models could be disseminated more.[29]

17. The City of London Police has the national leadership role for fraud, and looks to work with other forces, telling us that it had a range of ongoing activities. For example: it sends an infographic twice a year to each force with a breakdown of fraud related data for their area; has an ongoing programme of peer reviews to give advice on dealing with fraud, and had done 27 reviews so far; has best practice guides available and often sends out advice on prevention and protection. But the City of London Police stressed to us that decisions on what a force will prioritise are local, with local accountability. Therefore it

23 C&AG's Report, para 17
24 Qq 97–98
25 Q 169
26 C&AG's Report, para 10
27 Q 112
28 Q 43; Correspondence with Age UK, 26 October 2017
29 Q 49

cannot mandate actions to other forces, which are balancing referrals on fraud against all their other areas including, for example, public protection, modern slavery, and domestic abuse.[30]

18. We put it to the City of London Police that, despite its encouragement of other forces, the response from local forces remained inconsistent. The City of London Police Commissioner reiterated the difficulties for forces of competing demands and the need to tackle the most serious crimes, but he also commented that "the Joint Fraud Taskforce, however perfect or imperfect it may be, has raised the profile of this crime type, without a doubt in my view, across law enforcement, across businesses and across government".[31] The City of London Police also told us that, for law enforcement, part of what success would look like in tackling online fraud would be for there to be greater consistency across law enforcement.[32]

30 Q 112
31 Q 167
32 Q 169

2 The role of banks and awareness campaigns

19. Banks have an important role to play in protecting customers against fraud. However, the protection banks provide varies, with some investing more than others in customer education and anti-fraud technology. The Payment Systems Regulator has found that banks needed to improve the way they work together in responding to scams, that some banks needed to do more to combat scams, and that data available on the scale of scams were poor. Which? has argued that shifting liability for scams onto banks would encourage them to protect their customers better.[33]

20. UK Finance told us that online fraud is a problem that the industry takes incredibly seriously.[34] The Chief Executive commented "I would say we are succeeding" based on his figure that total fraud had gone down 8% while transactions have been increasing, but also acknowledged that there is more that the industry can do.[35] Age UK told us it would like to see banks doing more to help vulnerable people, for example on putting restrictions on their bank accounts which maintain financial independence for them, but make them less vulnerable to the risk of losing huge amounts of money. UK Finance said it was identifying practices across the industry, in particular on withdrawing some online functionality for customers where it was not needed.[36]

Data on banks' performance

21. We asked representatives of the finance industry why the only data made available of incidents of fraud was at aggregate level, rather than by individual banks. Customers at the moment do not have any information on which banks are performing better on this than others. UK Finance said that seeing where patterns are emerging at the aggregate level was helpful for the industry. Lloyds told us that individual banks know how they compare with others, but told us that banks did not publish individual numbers because then the fraudsters would target the 'weakest' of the banks.[37] We suggested that it might be in the banks' own interest not to be transparent and publish individual data, as it could deter customers. Both UK Finance and Lloyds maintained that the negative effect, of potentially revealing to fraudsters where they should go, was the more dominant argument for them.[38] We do not find this a compelling argument. The experience of the car industry in relation to car theft was referred to by our witnesses—the publication of a car-theft index not only informed consumers, but also prompted the car industry to deliver improvements.[39] Rather than signposting weaknesses to fraudsters, we consider that greater transparency from the banks would ensure that those potential vulnerabilities in the system would be addressed as a priority, thereby improving, not reducing, security.

33 C&AG's Report, paras 11, 2.9, 2.10
34 Q 1
35 Q 45
36 Qq 18–19
37 Qq 2–4
38 Qq 21, 22
39 Qq 79, 129

22. We understand that Age UK has suggested a league table of banks' performance and Age UK confirmed that, in its view "there is a strong case for greater transparency."[40] The Department told us that at present the data available to it is not good enough to support publishing a table that ranked the banks. It said that, while it was not Government policy now to have such a table, that did not mean it was ruled out for the future.[41] In fact the Department confirmed that it did not currently see data on the relative performance of banks at all.[42] Even the City of London Police does not see data showing it which particular banks have got more or less of particular kinds of fraud—it told us that such data would be intelligence from which it could look at what action to take, would be used for tackling crime and not for any other purpose, and that confidentiality would be respected.[43] There is no formal requirement for banks to report fraud or share reports with government.[44] It is also not mandatory for a bank to notify cases to Action Fraud, although the Departments told us there is a "strong expectation" that they would do so.[45] The City of London Police confirmed that, if it had access to individual banks' figures, that would give it a pretty accurate view of how much was actually getting through to it.[46]

Card not present fraud

23. Criminals using stolen card details to make fraudulent transactions, including over the internet, is known as 'card not present' fraud. Known cases of this type of fraud increased by 103% between 2011 and 2016, from 709,000 to approximately 1.4 million incidents.[47] The Department told us that card not present fraud, along with funds repatriation, were the two things it was prioritising with the banking sector and financial institutions.[48] It said that, through chairing a recent oversight board meeting of the Joint Fraud Taskforce, the Home Secretary had vigorously held Mastercard and other representatives of the private sector to account for delivering as quickly as possible a technical solution to card not present fraud. The Department told us that it wanted to see "a very significant reduction" in card not present fraud by 2019, though could not quantify more precisely what reduction it expected to see "because it will depend on the solutions that are arrived at".[49]

24. We asked whether banks could make better use of technology to tackle the problem, for example using changing CVV numbers on cards. Lloyds told us that very few banks are using changing numbers, and that if the sector were to move towards doing so then it would have to be an industry initiative that everybody did at the same time.[50] Lloyds stressed the work that banks were doing 'behind the scenes', for example investing in tools to help them identify riskier transaction, that was not visible to the consumer. It told us that consumers want faster and faster banking services and that, while banks could intervene more and put stops on lots of transactions, that would interrupt the flow of transactions

40 Q 18
41 Qq 80, 81
42 Qq 86
43 Qq 87–92
44 C&AG's Report, para 17
45 Qq 77–78
46 Q 105
47 C&AG's Report, para 7
48 Q 136.
49 Qq 94, 137
50 Q 56

and of banking.[51] The Department also stressed the need for industry-wide solutions, in general to fraud, but also specifically to deal with card not present fraud—"That is really only likely to be delivered effectively if we have industry-wide co-operation".[52] The Department told us that, through the Joint Fraud taskforce, it was discussing the scope for designing out crime opportunities and designing in protection at the very earliest stages of the development of new technology.[53]

Funds repatriation

25. Banks are reported to be holding at least £130 million of funds that cannot accurately be traced back and returned to fraud victims, an amount that UK Finance said was probably a conservative estimate. UK Finance also told us that the amount represented frozen funds, believed to be connected to fraud, where banks have identified a concern and started to investigate further, which had caused the National Crime Agency or the police to freeze the money within the accounts. It was therefore not for the banks to say what happens to that money, because it has been frozen by the judicial system.[54]

26. Lloyds said that the main emerging threat was 'authorised push payments' whereby the customer asks the bank to move money, but has been the victim of a scam convincing them to do so.[55] Age UK drew our attention to a variety of scams where victims had been convinced to transfer money, and to the distress caused as well as the financial losses.[56] It has been estimated that between 40% and 70% of people who are victims of scams do not get any money back.[57] Lloyds told us that different banks would have their own appetite for judging whether to refund customers, but that Lloyds would look at whether an individual had taken "reasonable steps", such as to verify who they had been talking to and not being reckless with their information, and would also take account of whether Lloyds had given them a warning. Lloyds said that someone is far more likely to obtain a refund if a vulnerability has contributed to them being scammed.[58]

27. The Department told us that it was taking forward a major initiative with the banks on funds repatriation, for a much better system which could potentially deal with quite a significant proportion of authorised payments. It said that a system making the best use of technology to spot 'mule accounts' (accounts which exist for the purposes of channelling monies obtained through fraud) and repatriate money quickly could provide a lot of consumer protection. The Department added that being able to track money back through multiple mule accounts, freeze it and return it to the victim could also improve intelligence about the mule network and better assist law enforcement. The Department highlighted that there may be legal challenges to such a system and it needed to work through the legal protection that the banks were asking for, and so it thought it would be "a couple of years" before it had a fully fledged programme. It did say it would press the banks to see whether there are some classically quick wins it could do well before that to "demonstrate the proof of concept".[59]

51 Q 47
52 Q 81
53 Q 120
54 Q 53; C&AG's Report, para 11
55 Qq 6, 7
56 Correspondence with Age UK, 26 October 2017
57 C&AG's Report, para 11
58 Q 52
59 Qq 145, 146

Awareness campaigns

28. Many people are still not aware of best practice for keeping safe online and there is more to do to help citizens' and businesses improve their cyber security.[60] The City of London Police stressed the importance of investing time in prevention and the education of the public.[61] Age UK told us there was huge scope to do much more to help prevent people from being victims, stressing also the importance of making sure people who have been victims in the past do not become victims again.[62]

29. While there is a perception that online fraud primarily affects the elderly and vulnerable, young people are increasingly likely to fall victim. Social media plays a significant role in online scams and further education is needed to make young people aware of the dangers of sharing personal information online. The City of London Police told us that young people are probably more vulnerable to fraud than older generations as they have a very different approach to personal information. The City of London Police cited examples of young people sharing pictures of their passports and driving licences on social media.[63]

30. The government and other bodies run various campaigns; in March 2017 there were more than 10 different ones running at the same time. There is a risk that different organisations running campaigns with slightly different messages not tailored for specific groups can confuse and reduce impact.[64]

31. UK Finance also highlighted the importance of education in helping people not to become victims, mentioning in particular the 'Take Five' campaign. Take Five has been going for a while, but was relaunched two weeks before our evidence session, with the slogan "My money? My info? I don't think so".[65] Recently the Department provided £500,000 towards the campaign, out of total funding of £3.8 million.[66] The Department said that success for the Take Five programme would be "measurable improvements in behaviour, with people being confident enough to say no and to challenge when fraudsters are after their money".[67] The Department is evaluating the success of the Take Five campaign, though results are not due until March 2018.[68]

60 C&AG's Report, para 13
61 Q 100
62 Q 40
63 Q147
64 C&AG's Report, para 13
65 Q 26–33
66 Qq 140–142; C&AG's Report, para 3.7
67 Q 142
68 Q 142; C&AG's Report, para 3.7

Formal Minutes

Monday 27 November 2017

Members present:

Meg Hillier, in the Chair

Luke Graham	Nigel Mills
Gillian Keegan	Layla Moran

Draft Report (*The growing threat of online fraud*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 31 read and agreed to.

Introduction agreed to.

Conclusions and recommendations agreed to.

Summary agreed to.

Resolved, That the Report be the Sixth 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 Wednesday 29 November 2017 at 2.00pm

Witnesses

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

Wednesday 18 October 2017	*Question number*
Jane Vass, Head of Policy and Research, Age UK, **Stephen Jones**, CEO, UK Finance, **Brian Dilley**, Group Director of Fraud & Financial Crime Prevention, Lloyds Banking Group, and **James Martin**, Crime and Security Adviser, British Retail Consortium	Q1–56
Philip Rutnam, Permanent Secretary, Home Office, **Richard Riley**, Director for Serious and Organised Crime, Home Office, and **Ian Dyson**, Commissioner, City of London Police	Q57–169

Published correspondence

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

1 Correspondence with Age UK relating to online fraud

2 Correspondence with Cifas

3 Correspondence with the Home Secretary relating to the Committee's inquiry on the growing threat of online fraud

4 Correspondence from UK Finance relating to Online fraud

5 Evidence from Which? regarding the Growing Threat of Online Fraud

List of Reports from the Committee during the current session

All publications from the Committee are available on the publications page of the Committee's website.

Session 2017–19

First Report	Tackling online VAT fraud and error	HC 312
Second Report	Brexit and the future of Customs	HC 401
Third Report	Hinkley Point C	HC 393
Fourth Report	Clinical correspondence handling at NHS Shared Business Services	HC 396
Fifth Report	Managing the costs of clinical negligence in hospital trusts	HC 397
First Special Report	Chair of the Public Accounts Committee's Second Annual Report	HC 347

HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: The growing threat of online fraud, HC 399

Wednesday 18 October 2017

Ordered by the House of Commons to be published on 18 October 2017.

Watch the meeting http://parliamentlive.tv/Event/Index/3ca30053-8736-44f3-a63c-a1ffeb055e3a

Members present: Meg Hillier (Chair); Geoffrey Clifton-Brown; Martyn Day; Chris Evans; Caroline Flint; Luke Graham; Gillian Keegan; Shabana Mahmood; Nigel Mills; Layla Moran; Gareth Snell.

Sir Amyas Morse, Comptroller and Auditor General, Adrian Jenner, Director of Parliamentary Relations, National Audit Office, Linda Mills, Audit Manager, NAO, and Richard Brown, Treasury Officer of Accounts, HM Treasury, were in attendance.

Questions 1 - 169

Witnesses

I: Jane Vass, Head of Policy and Research, Age UK, Stephen Jones, CEO, UK Finance, Brian Dilley, Group Director of Fraud & Financial Crime Prevention, Lloyds Banking Group, and James Martin, Crime and Security Adviser, British Retail Consortium.

II: Philip Rutnam, Permanent Secretary, Home Office, Richard Riley, Director for Serious and Organised Crime, Home Office, and Ian Dyson, Commissioner, City of London Police.

Written evidence from witnesses:

– [Add names of witnesses and hyperlink to submissions]

HOUSE OF COMMONS

Report by the Comptroller and Auditor General

Online Fraud (HC 45)

Examination of witnesses

Witnesses: Jane Vass, Stephen Jones, Brian Dilley and James Martin.

Q1 **Chair:** Welcome to the Public Accounts Committee. We are here today to look at online fraud. We have two panels and are working off some of the information from the National Audit Office's excellent Report into this growing threat. We will later have Government figures who are helping to tackle this but on our first panel we have a mixture of people both representing consumers—I suppose, in a way, you all represent consumers—and at the forefront of tackling this.

From my left to right we have Jane Vass, the chief executive of Age UK—

Jane Vass: Director of policy and research.

Chair: Forgive me; she is the director of policy and research at Age UK. I have a list that gives you different titles from those under your names; I will double-check it before we introduce you wrongly. We have James Martin, the crime and security adviser at the British Retail Consortium, Stephen Jones, the chief executive officer of UK Finance, and Brian Dilley, the group fraud and financial crime prevention lead at Lloyds Banking Group. Welcome to you all. We are aiming for this session to last about half an hour, so if you could keep your answers short and to the point, that would be incredibly helpful.

May I start with Stephen Jones from UK Finance? One of the interesting things about this hearing is that we did not really receive any evidence from banks and financial institutions about the problem. I wondered whether there was a reluctance for them to admit any fraud that is going on that they are aware of, or do you think they just didn't feel like submitting evidence?

Stephen Jones: I am sorry; I do not know why evidence wasn't formally submitted, but it is a problem that the industry takes incredibly seriously. As you know, we currently publish the data on unauthorised fraud and are about to start publishing the data on authorised fraud in a manner that ensures that we can—

Q2 **Chair:** But that is published in aggregate, isn't it, and not by individual banks?

Stephen Jones: It is not published by individual institutions at the moment. At the end of the day, I think seeing where patterns are emerging in aggregate is helpful from an industry perspective. There may be divergences between individual institutions; part of our job at the centre, as the trade association, is to try to highlight that and ensure that best practice is promulgated across the membership, in order to make

sure that everybody is performing to the highest level, rather than the lowest level, frankly.

Q3 **Chair:** Mr Dilley, does Lloyds Banking Group publish any information as a group?

Brian Dilley: We publish information around our approach to fraud prevention. We don't publish numbers.

Q4 **Chair:** Why not?

Brian Dilley: One reason the banks don't publish individual numbers is because, if you could compare the numbers and see which was the weakest of the banks, that is where the fraudsters would go.

Chair: You might also lose customers.

Brian Dilley: You may do.

Q5 **Chair:** Is that a consideration?

Brian Dilley: It would encourage the fraudsters to direct their activities towards the weakest area. Each bank knows how they compare; they know their own numbers compared with the industry numbers. We know how we perform against others, and that is used internally to improve our processes.

Q6 **Chair:** So what is the biggest problem for Lloyds Banking Group? What is the biggest, latest issue that you are hitting?

Brian Dilley: I think the emerging threat is authorised push payments—the authorised fraud. As we improve our controls over unauthorised access and we improve those mechanisms, the fraudsters are moving towards scams. From our perspective, that presents itself as the customer asking to move the money.

Q7 **Chair:** Do you give the money back? Have you ever given money back to anyone who has been the victim of that sort of thing?

Brian Dilley: We do give money back in certain circumstances, but not in all circumstances, because there is a limit to what we can do to prevent that. There are plenty of examples of where we have warned a customer that we think it is a scam but they insist on us processing the payment. By law, we have to process the payment.

Q8 **Chair:** Are there many people who are warned by the bank that it is a scam?

Brian Dilley: It does happen surprisingly regularly.

Q9 **Chair:** Percentage-wise?

Brian Dilley: I do not know the answer to that, percentage-wise.

Q10 **Chair:** What about if I were to walk into a Lloyds bank—I am not picking on you, but you are here representing one institution—and suddenly say I want to withdraw all my savings, what would your staff do about that?

The online bit might have happened, but the actual financial transaction may be a physical one.

Brian Dilley: Within the branch, we have a very good record of preventing those types of payments. We have spent a lot of time training our staff on what to look for. Where there are indications that somebody may be making a transaction under duress, or because somebody has told them to, there is an additional set of questions. I also think the banking protocol has been a very big success. That is where, in the branch, they can call the police, who will come around and who often arrest the fraudsters, if the fraudsters are with them, or stop the individual making a payment.

Q11 **Chair:** You say you are doing very well on that. Can you give me some precise examples or figures for how you can prove that you are doing very well?

Stephen Jones: The banking protocol is one of the tangible outputs of—

Chair: That is the protocol. I am talking about when you say you stop people coming in and doing a fraudulent—

Stephen Jones: I was going to give you the numbers from the banking protocol, which is the recent cross-industry—not just Lloyds bank—initiative.

Q12 **Chair:** The banking protocol is getting the fraudster in the bank, isn't it? I was talking about when someone comes in to withdraw their life savings or some uncharacteristic transaction. Mr Dilley, you said—forgive me if I misunderstood you—that you had a good track record on dealing with that in branch. Can you give me some examples? When you say you have a good track record, how can you prove that? Can you give us some more examples about how you have done that and what numbers you have been catching in branch, relative to other banks?

Brian Dilley: I think the banking protocol is relevant to that, because it is about those situations. If you have a situation where somebody comes in to transfer their life savings, and the teller in the bank thinks there is something suspicious, they will phone the police at that point. Those are examples of preventing real fraud.

Q13 **Chair:** You say you are doing very well on that. Do you think you are doing better than other banks?

Brian Dilley: I do not have the split by bank.

Stephen Jones: We are in the middle of rolling out the campaign nationally. So far, it has been rolled out with the police across 22 police forces, about halfway across the country. It started at the beginning of this year; by August 2017, about 900 cases had been referred to the police and about £6 million of fraud prevented as a result of staff being given specific training to identify duress in customers approaching tellers, and of the tellers physically intervening and calling the police to prevent

the customer from withdrawing the money, even though that was what the customer had expressly come into the bank branch to do.

Q14 **Chair:** People coming in under duress to take their money out is quite a small subset, isn't it? What about people who come in without apparently being under duress, who have been scammed at an earlier point online and asked to take the money out?

Brian Dilley: We have a whole set of criteria that we train our bank staff to look for. It is not just whether they are under duress, but if they ask to empty their account, for example. I do not want to go through all the individual examples, because then the fraudsters will avoid doing those things, but there is a whole list of things that could give rise to additional questions, to the banking protocol or to warnings to customers that we think it might be a scam.

Chair: Mr Evans, do you want to pick up on this?

Q15 **Chris Evans:** I should declare an interest as a former member of staff of Lloyds TSB, as they were then. My question is quite straightforward. You are closing numbers of branches all over the country. You say that the branch network is a stop on potential fraud. As you move from a branch model into more of an internet-style model, which I can perhaps understand, how are you guarding against people being under duress online?

Brian Dilley: We are doing a number of things around identifying transactions that look like they might be suspicious. To give you two examples of what Lloyds have done, we have added a box on to the online banking that will tell you which bank it is when you put the sort code in. That has stopped a number of them, because often people say "Transfer it to another account at the same bank," and this comes up and shows you that it is a different bank.

This month, we are going live with some additional questions when you set up a new payee, which also have a number of educational aspects, saying, "If you have been asked these things, this might be a fraud," and asking you to confirm that you have not done certain things. Behind the scenes we have analytical tools to try to look for transactions with certain characteristics that might indicate that they are authorised push payments.

Q16 **Chris Evans:** I know you have left the regulated market now, but there was a huge problem of fraudulent mis-selling. How have you clamped down on that in the years since I left the bank?

Chair: Please be very brief on this, because it is not quite the same question.

Chris Evans: I could give you a number of examples of where people were put into bonds that they were told were savings accounts, and things like that. How have you cut down on fraudulent mis-selling? If somebody is found to be fraudulently mis-selling, what punishments are available to you there, besides dismissal?

Chair: Mr Evans, you have made your point, but we need to move on. You can answer the question, but then we will move on.

Brian Dilley: That is not an area of my direct responsibility, but the whole—

Chris Evans: Perhaps Mr Jones has an idea on fraudulent mis-selling?

Stephen Jones: The fraud you are pointing to is fraud by bank staff themselves in mis-selling.

Chris Evans: Yes, mis-selling. There have been a number of—

Chair: That is not quite the same as online fraud, Mr Evans.

Stephen Jones: There is a huge issue. We could spend the whole Committee talking about it.

Q17 **Chair:** Yes; if you could just answer the question as briefly as you can, then we will move on.

Stephen Jones: There is significant effort being undertaken to prevent bank staff from undertaking fraud on their customers. A huge amount of the conduct agenda over the last 10 years has been focused precisely on that agenda, and there is a significant amount of time, money, effort and, frankly, passion and heart going into making sure that that does not happen in the industry.

Chris Evans: That is what I was looking for; thank you.

Q18 **Layla Moran:** Sticking with the theme of what banks can do more of, I will bring you in, Ms Vass. I understand that Age UK have suggested a league table of banks. Can you tell us why you have come up with that suggestion?

Jane Vass: We would certainly like to see more transparency. I think the main thing for us—as well as things like the branch protocol, which is valuable and important—is that banks look at helping people who might want to put restrictions on their bank accounts if, for example, their mental capacity is declining, to allow them to maintain their financial independence and do what they can; they are not open to major risk of losing huge amounts. That is really what we would like to see banks do.

In terms of banking transparency, we want to see the banks do more and come up with many more suggestions like this that will meet the needs of vulnerable people. But obviously if there is not enough action—Which? has come out with its authorised push payment super-complaint—there is a strong case for greater transparency.

Q19 **Layla Moran:** So, for the vulnerable users of your banks, don't you think it is only fair that they and their families have access to all data and that, if there were a league table of which banks are less secure than others, they deserve to have that?

Stephen Jones: If I could put it more positively than that, actually what we are doing is going across all the members in the industry to identify exactly the kinds of practices that Jane has highlighted: in particular, ironically, where you are withdrawing functionality from clients online because they are not confident that they need that functionality and they are concerned about their vulnerability if that functionality is left available to them.

Q20 **Chair:** This puts a lot of onus on the customer.

Stephen Jones: At the end of the day, it is possible that different products in an outright sense can be offered which are basic and simpler with less, but ultimately there is a discussion that needs to happen between the customer and the bank in terms of the level of service that they want, particularly where they have a particular level of concern about whether that exposes them to issues of vulnerability.

Q21 **Chair:** Mr Dilley, Ms Moran quite rightly pushed the point about transparency. Just to pick up what I was saying earlier as well, isn't it possibly the point that if you were more transparent—*[Interruption.]* It's the ghost of Gladstone. Sorry, I do not know why I got distracted by that. Isn't it the case that, as I said and Ms Moran has highlighted, if you reveal more about your position, it is not for your competition in attracting customers and, in effect, it helps you by not being transparent.

Layla Moran: It is a race to the top, surely.

Brian Dilley: As I say, the unintended consequence is that you reveal to the fraudsters where they should go first, and the fraudsters will move in an instant. Yes, it would have some competitive impact, but we do monitor what our customers are doing. We monitor complaints, to see whether that is causing individuals a problem in terms of how they are operating the accounts, and I think the negative side in terms of indicating where the fraudsters should go to would outweigh the competition aspects, which we do partly through things like FFA UK—*[Interruption.]*

Chair: I think we are all going to have to speak up. I am sorry. It is very distracting. We are trying to get it sorted out. It is either the wind—

Stephen Jones: You talk about the race to the top—

Q22 **Layla Moran:** A race to the top for security and safety. I am worried, now. You know if my bank is safe or not, but I do not. Shouldn't I?

Stephen Jones: The whole industry is increasingly built around the sharing of data and of risk across the industry and with the criminal agencies, the police force, the National Fraud Intelligence Bureau and our own Financial Fraud Bureau in order to ensure that where incidences of attack of fraud emerge, that data is shared quickly across the industry, the vulnerability that is being attacked is identified and it is stopped across the industry.

That approach has demonstrated some impact: there was an 8% reduction in cases of unauthorised financial fraud in the first half of this year

compared with the first half of last year. The number is still far too high, but there were 937,000 cases of fraud against 16.4 billion transactions. We monitor that very, very carefully and very closely, and we are seeking to share threats as they emerge, how they can be prevented and make sure that the prevention measures take place across the industry.

It is in our view better that that activity takes place in private, not in public, for the reasons that Brian has highlighted. It is not because we are trying to hide from the spotlight. At the end of the day, in the case of unauthorised financial fraud, this is a cost to the banks—the customer gets the money back—and it is therefore in the banks' interest to prevent this fraud as well. But that kind of triage involving the banks themselves and the criminal agencies sharing data and threat information is how we build defences to what is an ever increasing threat of fraud across the sector.

Q23 **Layla Moran:** Except we have just been told that consumers do not always get their money back.

Stephen Jones: In the vast majority of unauthorised financial fraud cases, customers get their money back. In the case of authorised financial fraud, where a customer deliberately makes the payment—does so intentionally—and the bank is therefore obliged to effect the customer's instructions and make the payment, there are circumstances in which the customer does not get the money back, because all the bank has done is give effect to the customer's wishes to make a payment to a third-party account that that customer has nominated.

Q24 **Chair:** Okay. People are very interested in coming in, so Comptroller and Auditor General Amyas Morse, Mr Day and Ms Keegan.

Sir Amyas Morse: To be clear about this, given that you say the lack of transparency about individual bank performance is not as a result of banks not wanting to help themselves competitively or anything like that, does that mean, if you were clearly advised by Government or the anti-fraud authority that more openness would help, you would go along with that?

Stephen Jones: If the Government or the regulators instructed the banks to publish individual data on fraud, we would argue that that is not a very good anti-fraud prevention measure, but if the Government insist on that, we would have to publish it.

Q25 **Martyn Day:** Mr Jones, on your comment about sharing of risk, when we see figures to suggest that, with the unauthorised push payments, perhaps as many as 7% of people do not get their money back, clearly at the moment the risk is with the consumer, the customer. May I give you an example from my own constituency casework of the complex nature of some of the frauds we are getting? I have a few examples. I should say that these were not elderly or vulnerable individuals who would have considered themselves at risk; they would never have thought that they were in the voluntary at-risk category.

One young woman, who was an immigration case, received a call on her mobile phone that appeared to come from 999. She answered it and they pretended to be the police, knowing that she had an immigration case—

she needed to send a payment because they had 72 hours to go through the Indian embassy and everything. They managed to trick her into logging on to her computer and using TeamViewer, and they transferred what she had in her bank account to themselves.

In her case, she got the money back, but she got the money back because she had insurance. Surely that is another example of the risk being transferred to the consumer and you not being protective yourselves. How could you help people in that situation?

Stephen Jones: I hope I did not use the term "risk transfer", because that is not the way we think about it. Every case of fraud is a personal tragedy and a case that we need—

Chair: Sharing risk, I think you said.

Stephen Jones: I also want to clarify: in the vast majority of cases of unauthorised fraud, money is returned to the customer. In cases of authorised push payment fraud, as the jargon goes, where someone deliberately inputs the instructions and says, "Please make the payment to this person", for whatever reason—in the case of your constituent, unfortunately, she was led to believe by a 999 call that that payment was appropriate—not all proceeds are returned to the customer, because the bank has simply been acting on the customer's instructions.

Q26 **Martyn Day:** In that particular case, the individual was referring to the TeamViewer person doing it, rather than doing it themselves. However, another example, which is more on the push payment approach, is Mrs Galloway, in my constituency—again, this was exactly the same kind of person, perfectly switched on; you would not identify her in any way as being vulnerable. She had a virus on her computer. She noticed that emails appeared to be coming in already opened. She contacted her net provider. They ran checks on her line and came to the conclusion that they could not see anything. Then she got a fraudulent call pretending to be from the internet adviser and getting her to run a piece of software, which obviously gave them more information. While she was on her computer, they transferred money between her own bank accounts, from her savings to her main account, and then she got the call to say there had been an erroneous payment into her account. She checked, and there was the best part of £4,000, which should not have been there. The people asked her to send it back to them. Of course, she then effectively authorised a push payment, lost all that money and did not get a penny back. That is a real problem in the real world.

From the consumer's point of view, their bank account has been tampered with, without them having made the transaction. Obviously, that was not the push payment transaction, but there was a still a transfer that they did not make, which then led them to believe there was a genuine problem. How do we help people in that position?

Stephen Jones: The first thing is education. Within UK Finance, we operate Financial Fraud Action UK. The Take Five campaign, which we run jointly with the Home Office and is funded largely by the industry, is entering its second phase.

Q27 **Chair:** Take Five was relaunched, interestingly, on 2 October.

Stephen Jones: It was, yes.

Chair: That was interesting timing.

Stephen Jones: Well, it was the timing that was agreed with the Home Office.

Q28 **Chair:** Okay. We did a little litmus test around the Committee Room. Perhaps we are not an average bunch of people—I don't know. Probably not—we are a bunch of politicians, after all—but none of us knew what Take Five was. Could you tell us, Mr Jones—you've probably got it written down there—what the slogan is for Take Five?

Stephen Jones: Yes. "My money? My info? I don't think so."

Q29 **Chair:** Okay. I wonder whether anyone in the—well, I can't really do an audience litmus test, because it is not that kind of meeting.

Stephen Jones: That is slightly unfair, because you are highlighting a campaign that has been in action for two weeks. Even if you went to Procter & Gamble in two weeks, they wouldn't have managed to—

Q30 **Chair:** But Take Five has been relaunched. It was around before. It is only a £3 million programme, isn't it? How much of that was from the private sector?

Stephen Jones: Three point eight million pounds is being spent in the second phase of the programme. Most of that is from the sector. That does not take into account what individual banks are spending in order to promote the Take Five brand as a campaign within the institutions.

Q31 **Chair:** Right, Take Five the brand. So that £3.8 million was—

Stephen Jones: That is the central spend.

Q32 **Chair:** That is the central spend, and then—

Stephen Jones: Then each of the members is using Take Five as the collateral to support their anti-fraud education campaigns up and down the network. I think you will see significant activity over the next three to four months.

Q33 **Chair:** But how long has the Take Five brand been around? It has not been just two weeks, has it?

Stephen Jones: No, the initial campaign—Brian—was started 18 months ago.

Brian Dilley: Yes, 18 months ago.

Q34 **Chair:** It is interesting that none of us had heard of it. Okay, we are perhaps not a bunch of random people. I do not know whether we are a good litmus test, so it is perhaps not fair to highlight that.

We have left Mr Martin for a little bit. Mr Martin, what is the scale of fraud in your sector?

James Martin: Thank you. One of the products the BRC produces annually is a retail crime survey.

Chair: Sorry, could you speak up? For a room built for speaking, it has terrible acoustics.

James Martin: Of course—I will try not to shout. Annually, we produce a retail crime survey, which looks at the experiences of crime among our members. This year, we surveyed something like 30% of the industry by turnover and employees. In terms of online fraud, the figure reported to us was around £100 million direct cost to retailers, which is quite significant.

Q35 **Chair:** Cost to retailers?

James Martin: To retailers. That is the cost they bear.

Q36 **Chair:** Do you measure the cost to customers?

James Martin: We don't necessarily have that in our figures, no. It may not be reported in the same way, and it may be, of course, that the retailer does not actually know that. They are transferring the information in terms of the report, but they do not see the end result in terms of who is refunded by a bank, so it is not something they necessarily have. But that is the kind of scale that they see. What that does not take account of is the spending in terms of prevention and protection. Retailers take a very active role in this and deploy some fairly—*[Interruption.]* Sorry, it has started whistling again.

Q37 **Chair:** I don't know whether that is an endorsement of what you are saying by the ghosts of the House of Commons or not.

James Martin: Retailers deploy some fairly sophisticated technologies to try to combat and root out fraud, and to stop fraudsters in advance.

Q38 **Chair:** What about information sharing? If I were to buy a knife, it would very quickly be recorded that I am a middle-aged woman with a track record that shows I am over 18. If my teenage daughter were to try to buy a knife, it would show quickly, through background checks, that she couldn't do that. Do you have similar background checks and data sharing with various bodies, including Government sources, as extra insurance against fraud?

James Martin: Yes, of course. Without going into too much detail because of the risk of alerting people, there are all sorts of databases and systems that look at patterns of unusual transactions or transactions that use questionable information and will flag that so that they can potentially be stopped and investigated. I spoke to a room of our members, who include some of the biggest retailers, this week and pressed them pretty hard. They were comfortable that they stop something in the region of 90% of the attempts they see. That is purely online.

Q39 **Chair:** There is an alphabet soup of organisations involved in combating fraud. Do you feel the sharing goes wide enough? Are there any bits of Government or business that are not sharing useful information about

known fraudsters or patterns of behaviour that you could easily do some checks on?

James Martin: The retailers are in a good position, and that is improving. We have a very good relationship with the Home Office. We sit on the Joint Fraud Taskforce, and we are being involved in developing some of those systems. There are some issues in terms of how reports can be made through the Action Fraud system and whether sufficient information comes back from that to retailers. That has been a reasonably difficult issue over a period of time.

Q40 **Chair:** Let me turn to Age UK. Do you think that there is enough information sharing? Do any of your members have any issues? For example, if they have been the victim of a scam, do you think enough is being done to prevent them being a victim in future?

Jane Vass: No. We think there is huge scope to do much more in this area. We have a number of projects going. For example, we have a project that is about to start next year, where we will receive referrals, working with Action Fraud, so that we can support individuals who have been victims in the past, to stop them becoming repeat victims.

Q41 **Chair:** How will that happen? Will Action Fraud alert you to individual named cases and you will refer that through your network?

Jane Vass: Yes, and then we will put them in touch with face-to-face befrienders, so that if the underlying problem is loneliness—if they are being groomed or whatever—you can go in and give that practical and emotional support.

A number of local Age UKs also have programmes with scams hubs locally. That works well where victim, trading standards and police work together. Then they can, again, support people who have been repeat victims of fraud. Obviously, that is all after the event.

Q42 **Chair:** Absolutely. We should just highlight that the highest likelihood of being a victim is you are under 65, a professional with a degree.

Jane Vass: Yes.

Q43 **Chair:** You are here from Age UK but you are actually not representing the most likely victim these days, although people might be surprised to hear that. You have a national organisation. You talk about trading standards and that varies across local authorities. Police would really only get experience, as the Report highlights, in Sussex police and the City of London police, who are doing good work on this. What is your view? Is it as patchy as the Report suggests?

Jane Vass: It is extremely patchy. It depends geographically. In addition, we have talked to a number of individual banks and there has been action from individual banks but we would really like to see much more Government prioritisation of online fraud that would mean, for example, that where fraud is particularly targeted at vulnerable groups, it would take into account the impact on the victim, not just the amount of money. Because we have known cases where people have stopped using their

computer, unplugged their phone and, in the worst case, may end up in a care home earlier than they need to.

Chair: Thank you. Ms Keegan.

Q44 **Gillian Keegan:** Having spent much of the 1990s in the far east sorting the chips for chip and PIN, I worked for both a bank and payment system. This is always an issue, to try to keep one step ahead of the fraudsters, and technology is a massive part of combating that. If I look at some of the ways that you use technology today, it is kind of low-tech, a lot of the stuff that you are doing, such as CVC numbers and that kind of stuff. What are you doing now to get ahead? This can only grow; you have got all of the ingredients for this to be massive. What are you doing in terms of technology and investment in technology to protect your customers?

Brian Dilley: Any awful lot of what we are doing is not visible to the consumer because it is the things we are doing using artificial intelligence, machine learning and so on, to try to look for patterns in the data and try to identify the suspicious transactions. Banks are spending tens of millions of pounds a year on these systems to try to do exactly that.

Q45 **Gillian Keegan:** They are not very successful then, are they?

Brian Dilley: We are succeeding, actually, because the total level of fraud has gone down 8% while transactions have been increasing. I would say we are succeeding. Is there more that we can do? Yes.

Chair: But it's the largest growing area of crime, isn't it? Like it or not, you and your competitors—the people that Mr Jones represents—are at the forefront of the largest growing area. You are effectively on the ground the buffer between the customer—

Q46 **Gillian Keegan:** And have enabled it in a way.

Brian Dilley: If there are transactions there are going to be fraudsters. If there is money there will be fraudsters. Absolutely, we are at the forefront of that.

Q47 **Chair:** Do you have an ambition about where you want to be? In your own bank, you won't tell us how much fraud is going on—you could share it now, if you want. If you won't tell us that, will you at least tell us what your ambition is and about how you are trying to reduce the level of fraud in your bank and by what percentage? Do you have a target every year or two years? I know it is a moving target but you must have some target that you are setting internally.

Brian Dilley: Yes. We measure ourselves on three factors. We measure ourselves on our market share of losses and the absolute value of those losses; the customer experience; and the efficiency of our operations. Those are our losses—what we pay out—but customer experience is very important to Lloyds as well, because, essentially, we could put lots of stops on lots on lots of transactions and intervene a lot more, but that will interrupt the flow of transactions and the flow of banking. Legislation and

consumers want faster banking, faster payments and faster transactions. We are investing in tools that enable us to identify the riskier transactions, and we are looking for other authentication behind the scenes, which enables us to look at connections with trusted devices to blacklist devices that have been used for fraud and so on. All of those things are contributing to reductions in crime. You would not see all of those things as a consumer; chip and PIN is very visible to a consumer, whereas a lot of these things are behind the scenes.

Q48 **Chair:** Mr Martin, are retailers doing anything, technologically?

James Martin: I think it is a very similar pattern, in terms of how they operate. One thing to bring out is that they are not always passive or defensive; plenty of retailers operating with the authorities and, I am sure, other financial institutions, will seek to take down websites that are being used to effect and facilitate fraud. It is not just that they are trying to stop things as they enter their system. Once they spot these things, they will step out and try to find ways to stop that from happening in future. I think that is quite a positive role that they adopt.

Chair: Okay. We will have some quick-fire questions, because we only have about another five minutes. I will go to Mr Mills and Ms Keegan, and then I have two questions.

Q49 **Nigel Mills:** How would the panel rate the performance of City of London police, which has lead responsibility for this, and Action Fraud? Do you think they do a good job, or do you think they could be a bit more useful and helpful in tackling this crime?

Stephen Jones: In UK Finance, we operate the dedicated card and payment crime unit. That is a joint venture between City of London police and the Metropolitan Police that the industry pays for. We have found that to be extremely effective in on-the-ground crime prevention, detection and prosecution. Obviously, the best practice that is developed within that unit is then promulgated up and down the 42 other police forces in the United Kingdom. City of London police are at the forefront of enabling that to happen.

People have previously highlighted a patchy approach nationally, but having this central centre of excellence, with two police forces working together, is an extremely effective way of developing the best fraud detection techniques, which is what the unit is set up to achieve.

Nigel Mills: Ms Vass?

Jane Vass: The issue is not necessarily with City of London police, it is with pushing out that good practice around the country, so that we get action across the ground, rather than just depending on what happens to a report, which, at the moment, consumers and complainants don't actually know. At the moment, people are reluctant to report fraud because they don't think anything is going to happen, so you get a vicious cycle. We would like to see more consistent action, which is what older

people tell us: they want people there with teeth who can act on their behalf.

Chair: Mr Martin?

James Martin: The key touchpoint with City of London for my members is Action Fraud. I suppose I would start by saying that there are a lot of really good-quality people doing some incredible work there that is very useful. However, there are also some pretty serious systematic failings, in terms of block reporting systems and the information flow that comes back, which I think have been catalogued over some time. I know that City of London police are taking significant steps to try to remedy those, but I think they are slightly delayed in an IT project. We wait with bated breath to see how that improves, because that is an area in which we would like to see improvement. Again, that is not to say that there are not some absolutely excellent people doing some superb work.

Just to associate myself with the slight patchiness around the country once it has gone through Action Fraud, there are some examples of really good practice, such as Operation Falcon in the Met and so on, which do some really good things involving dedicated officers who are trained and deal with it properly. I know resources are very tight, but I suspect that those kinds of models could be spread a little bit more. One of the ways to do that may be to publish slightly more specific statistics and look at the standards and service levels and so on that are applied across the piece.

Chair: Mr Martin, you should be a member of this Committee; we love talking about transparency, statistics and data.

Q50 **Gillian Keegan:** It seems clear that, when the police start to roll out, the actual numbers are going to quadruple. That will mean that, once we have the numbers of how many people are actually suffering from this crime, your comments before about controlling it will be completely irrelevant. With that in mind, to give confidence and faith to consumers, you will have to be much more transparent with the actions and activities that you take, because this will balloon almost overnight.

Brian Dilley: To be clear, the numbers I was talking about were the ones that are within our control on transaction fraud. We know what those numbers are.

Gillian Keegan: As the payment technology providers, a lot of this is within your control.

Q51 **Chair:** Mr Martin, on that point of transparency, how much do retailers report on fraud in their area?

James Martin: In terms of individual retailers, I am not sure. We report an aggregate number, but the reason we are able to get a lot of the data, which is sometimes more business-sensitive, is that it is under some pretty strict confidentiality arrangements. There is also an issue in that retailers only see a small part of it, so it would be slightly misleading for them to publish bits of data over and above what they themselves pay out. It may be that the better way of looking at it is data from slightly

further up the system; whether that is aggregated or not, I am not quite sure.

Chair: Everyone is reluctant to reveal their own data, it seems.

Q52 **Shabana Mahmood:** In terms of banks paying out where an authorised payment has been made—a much smaller proportion of those individuals get their money back—what are the criteria by which you judge whether someone will get their money back or not? Do you treat different types of scams differently?

Brian Dilley: For authorised ones?

Shabana Mahmood: Yes.

Brian Dilley: Each bank will have their own appetite for that. I can tell you broadly what we do. We look at whether the individual has taken reasonable steps. In the example we heard earlier, we would look at whether that individual had taken reasonable steps to verify who they were talking to, whether they had been reckless with their information and so on. We take into account vulnerability, so someone is far more likely to obtain a refund if a vulnerability has contributed to them being scammed. We look at a whole range of different criteria in terms of individual circumstances, to say, "Has the person acted reasonably?" and then, "Have we given them a warning?" As I said earlier, we often give people a warning but they insist on proceeding. All those things will be taken into account.

Q53 **Martyn Day:** My question is for Mr Jones and Mr Dilley. There is obviously a lot more that everybody could be doing in this whole process. Currently we estimate that the banks are sitting on around £130 million of unreturned funds that they cannot source. What do you think should happen with that money?

Stephen Jones: One hundred and thirty million pounds is an estimate of frozen funds that are believed to be connected to fraud or fraudsters where banks have identified through their controls a concern and started to investigate further, which causes the NCA or the police to freeze the money within the accounts. It is not for the banks to say what happens to that money, because it has been frozen by the judicial system, but clearly the Joint Fraud Taskforce provides a useful public-private sector area where we can discuss it. Part of it could be used to create a pool for reimbursement. Part of it could be used to provide more resources to fight economic crimes in ways that the public sector deems most appropriate in the circumstances. I actually think that £130 million is probably a conservative estimate of what is stuck in the system, but it is not because the banks want to hold on to that money—I want to make that absolutely clear. It is because the banks are not allowed to do anything with the money under the way the law is currently set up.

Brian Dilley: The £130 million is not necessarily fraud-related. It is related to suspicious activity that has been reported by the banks. That could be all sorts of different crimes, not just fraud, and sometimes it is

not connected to an individual crime; it is just unusual transactions that have been reported. It is pooled money and then—

Chair: It underlines the need for transparency. If that could be broken down, it would be very helpful.

Q54 **Layla Moran:** We are about to talk to the Home Office reps. If there were one thing you could improve about working with the Joint Fraud Taskforce, what would it be? That question is to everybody.

Brian Dilley: We should recognise that the Joint Fraud Taskforce is a relatively young organisation. I would not disagree with the recommendation in the National Audit Office Report that now is the time to get some more formality to it, with some specific targets and measurements. I think it has achieved a number of good things, and it is time to move into a different phase.

Stephen Jones: A long-term goal is to take what has been a successful tactical association and affiliation to a permanent strategic public-private partnership. Public-private partnerships in this space are a really good idea. All stakeholders—retail, banking, representatives of the consumer and the vulnerable, the police, the National Crime Agency and the Home Office—working together on this problem is really important. Having long-term strategic goals would be useful.

James Martin: I think very similarly. It has clearly been a useful body and has come to a good point in its development. We now sit on it and have done for a few months, so I think they are probably thinking in the right way. We find that input very useful. I hope the Home Office does, but I'm sure that is not always the case. There is some really good co-working around things such as the implementation of the second payment services directive, which should give a really pragmatic approach in future.

Jane Vass: Public commitments to action, to which the committers can be held accountable.

Chair: That is what our job is, so thank you very much. I'm going to ask Mr Clifton-Brown to ask a last couple of questions.

Q55 **Geoffrey Clifton-Brown:** I have two very quick points. Mr Dilley, you have told us that all of your banks share the information. So is your bank, in proportion to its size, doing more or less than your competitors, and do you think your competitors could do more?

Brian Dilley: There is a range across different banks in terms of what the individual is doing. I tend to think that we punch above our weight. We do more than some others, but there are equally others around the table who are contributing a lot.

Q56 **Geoffrey Clifton-Brown:** So we shouldn't just be praising the best; we should be getting at the worst. Finally, we all know from our own constituencies, particularly those of us who represent rural ones, that you have embarked on a round of rural bank closures. Because we all know that you have saved a lot of transactional costs through the move to

online transactions, which has been considerable. Do you not think you could use more technology on the online transactions to try to tackle this problem more? For example, are all of the major banks now using changing numbers on their cards?

Brian Dilley: As I said earlier, we do an awful lot in terms of the transactional details. All the banks are not using changing numbers; in fact, very few are using changing numbers.

If we did move towards that, it would need to be an industry initiative that everybody did at the same time. The reason I say that is because there is anecdotal evidence that, it you have a changing PIN on a card, then consumers will often use the card with the PIN that they can remember—the CVV that they can remember—rather than going to get the card with the changing number. There are some aspects of consumer behaviour that move towards that sort of thing.

We have the same thing on 3D-secure, where you ask the additional questions. There are a number of dropped transactions when you come up with 3D-secure. Consumers often go, "I'll use another card that does not ask me those questions." So consumers often do move towards the less secure ones that are more frictionless.

Chair: You raise an interesting point about designing it out. If only we had more time. It has been a very interesting panel. Thank you very much for your time. The transcript of the whole hearing will be on the website uncorrected in the next couple of days. You will also be sent a copy. I urge you to send a correction if necessary. We had a report published today where a witness wrote notice yesterday that they did not agree with it, as it was about to be published, which was a bit late in the day. Do have a look at the transcript. Feel free to stay for the next session, if you wish. Could we change the witnesses and bring on the second panel, please?

Examination of Witnesses

Witnesses: Richard Riley, Philip Rutnam and Ian Dyson gave evidence.

Q57 **Chair:** Welcome back to the Public Accounts Committee on Wednesday 28 October 2017. Our hashtag today is #onlinefraud for anyone following on Twitter. This panel is people responsible for making sure that the country is trying to tackle this growing area of crime strategically. From my left to right, I am pleased to welcome Richard Riley, the director of serious and organised crime at the Home Office—welcome to you, Mr Riley. I am not sure if this is your first time in front of the Committee.

Richard Riley: It is my first time.

Q58 **Chair:** Welcome. We are a very friendly bunch, as you will discover.

We have Mr Philip Rutnam, Permanent Secretary at the Home Office, who is a regular visitor; he is back again in a few weeks' time. Welcome to you. We also have Ian Dyson, commissioner of the City of London Police.

We do not need to highlight too much the growing issue of online fraud—the report highlights it very clearly. It is now the most common crime in England and Wales; there were about 2 million incidents in 2016 alone. So it is big, but about 80% is not reported to the police. There is a really big issue here.

I'd like to start off with the Permanent Secretary. We heard quite a bit in that last session about the Joint Fraud Taskforce. It is a bit of a mystery to us—it's a bit of a "here today, gone tomorrow" event. Yesterday, we didn't have anything on it. At midday, suddenly up popped lots of minutes of meetings and so on. It was an unpopulated website until midday yesterday, and yet the organisation has been set up since February 2016. Do you take it very seriously?

Philip Rutnam: We take it very seriously. It is a very important innovation and a very important step forward.

Q59 **Chair:** Don't you think it is important that the public knows what is going on, if it is such an important innovation?

Philip Rutnam: I think it is very important that the public know what is going on.

Q60 **Chair:** So why wasn't the website working?

Philip Rutnam: I think with hindsight that information could in truth have been published rather earlier. Going forward, I would be very keen to see prompt publication of things like minutes of our oversight board and prompt publication to anybody who is interested of the very useful newsletters that come round. There is quite a lot we can do.

Q61 **Chair:** So it was not important enough for you to put information out there for the public to see. What happened? Was it an administrative glitch?

Philip Rutnam: I don't—

Chair: It is just that you are responsible for the security of the nation, in a sense—if I wanted to give you a grand title—and yet you can't make a website work.

Philip Rutnam: I think that is definitely over-estimating my importance. However, with hindsight, yes, there is more that we could have done to share that information earlier. In truth, we didn't give quite enough attention to the importance of sharing some of that information. Not everything goes perfectly. I think that the fact that we have got this Committee hearing today has helped in truth to focus minds—

Q62 **Chair:** To get the website working yesterday.

Philip Rutnam: What I would say, most importantly, is that going forward, we will make sure that we are sharing information such as the minutes of oversight board meetings promptly. I would say that there has been an awful lot of work going on in the Joint Fraud Taskforce, and an awful lot has been shared around that, but not through the website.

Q63 **Chair:** I think that people who aren't in those meetings but who are nevertheless interested, and organisations and individuals that have an interest, should be able to look that up.

It was interesting that a few hours after midday, some of the documents that had been uploaded were removed. Sadly, we didn't think to download them all because we didn't think they would be up there one minute and gone the next. I don't know if you know anything about why they would have been removed.

Philip Rutnam: You are ahead of me, Madam Chair. I have to say that I was not aware of that.

Q64 **Chair:** It just sounds a bit shambolic. This is a really serious issue and yet that simple thing of having that one website up and running—that one little bit of it—has not happened.

Philip Rutnam: I agree it is very serious.

Q65 **Chair:** Will you look into it?

Philip Rutnam: Of course I will look into that, and most importantly I would give the undertaking that going forward we will share the information that we can about the Joint Fraud Taskforce much more promptly.

Q66 **Chair:** There is a bit of a theme here—other colleagues will be picking it up—about how easy it is for people to get information online. One of the things to ask is who is ultimately responsible for making sure that consumers know what is going on. I have here a list of every organisation involved in online fraud. I haven't added it up, but it is probably 40 or 50 organisations. Of all of those, you are sort of at the hub. Are you responsible for making sure that online fraud is tackled? Do you want to take on that mantle or is it someone else?

Philip Rutnam: I think in fact the true list of organisations that are involved in some way, or have some interest in online fraud, would be much longer than that piece of paper—

Q67 **Chair:** We are being generous to you.

Philip Rutnam: It would be an enormous list. That is because every retailer and every financial institution in the country has an interest in this and many, many other organisations—

Q68 **Chair:** They have an interest, but some people have a responsibility.

Philip Rutnam: Our Ministers and I see our role as providing strategic national leadership for the country in responding to this challenge.

That does not mean that we do everything—far from it. It means that we have a critical role in making sure that there is a strategy that is prioritised and turned over time, in a suitably programmatic way, into action and results. We have a core role in relation to strategic leadership. As you say, we are at the heart—the hub, if you like—of the fight against this type of crime across the country.

Chair: You say that, but you have the misfortune of speaking in a room with two former Home Office Ministers, one of whom remembers the National Hi-Tech Crime Unit—that is Caroline Flint, who was there. Well, I don't know whether you were actually there at that time, Ms Flint. Do you want to pick up that point? Why don't you ask this question?

Q69 **Caroline Flint:** The National Hi-Tech Crime Unit was established in 2001, and it was merged into the Serious Organised Crime Agency in 2006—we have the National Crime Agency now—so this is not a new issue. I remember, having been the Minister for tackling organised crime, that part of the National Hi-Tech Crime Unit's job was to tackle issues relating to online fraud, computers, telecommunications, carding and all those other things. It has obviously morphed along the way, but the National Audit Office Report seems to indicate the same problems: a lack of joined-up thinking, a lack of good communications and a lack of sharing of best practice. The question is, 16 years on from the establishment of that unit, why are we still having to discuss these basic issues about good delivery of a service?

Philip Rutnam: I can't, in truth, speak to the past—certainly not with the same authority.

Caroline Flint: I always think that collective memory is a good idea.

Q70 **Chair:** I was the Minister responsible for identity cards, and part of my role was to look at online fraud. I had some good meetings with the City of London Police and others, and online fraud was launching about that time—2006, just before I became a Minister. There was lot of work and enthusiasm at the time, and it doesn't seem to have led anywhere, from what we have seen in the Report.

Philip Rutnam: I really don't think that is a fair characterisation of where we are now. As I say, I cannot speak to the organisational arrangements that have existed on this topic over the last decade or two.

Q71 **Chair:** But it is a growing area, and if we had been ahead of the curve—

Philip Rutnam: You are absolutely right that it is a growing area. That is one reason, together with the emotional harm it imposes on victims, the financial harm and the damage it does to confidence in our economic system, why we are taking it very seriously. It is unfair to say that we are not getting things moving in the right direction. That doesn't mean we have achieved everything—far from it. There is an enormous amount to be done. The NAO Report itself recognises that, in the Joint Fraud Taskforce and the strength of partnership that now exists between the Government, the private sector and law enforcement, we have made a good start.

Q72 **Layla Moran:** Mr Dyson, why is there such a large difference between the number of people affected by these calls and the number of reports to the police force? What is going on there?

Ian Dyson: I would say that there are three main reasons that fraud is under-reported. First, in many fraud cases, there is a sense of shame and a sense of, "I've been foolish." There is some research that says that the

word "scam" makes people feel that they have been duped, and it is something they are embarrassed about. Secondly, there is the challenge, which we touched on with the previous panel, that people report the loss to the bank, and if the bank recompenses them for the loss, they often do not report it to the police. Thirdly, there are some challenges relating to the efficiency of the reporting process. We have plans in place to address that.

Those are the three main areas we are looking at, and we have plans to look at all of them. Fraud is a modern crime type. It is global; it is big data. It is one of the few areas for which the significant amount of data is in the private sector, not in law enforcement. That is why the work that the Joint Fraud Taskforce is doing to encourage data sharing and intelligence sharing is so important. We have to move above thinking that we can enforce our way out of this problem. Enforcement is an important element—it is part of my role—but prevention and protection of the vulnerable are really important, too.

Q73 **Layla Moran:** Might I add that a further possible reason that people are not reporting to you is that they get the brush-off? I have got an example of a gentleman who had been scammed for the second time—this is the Microsoft scam, where they call you and say there is a problem with your computer. He had been caught out once. He knew that these guys were probably fraudsters. He called 1471 and in fact got the number. He then went to his local police station and tried to report the crime. They said that they absolutely could not take the report. He had to be turned away. They said, "Go and talk to Action Fraud." He then tried to talk to Action Fraud, which was apparently not open on weekends. I myself tried over a weekend—it is true that they do not advertise it, although in the online chat I was then told that they are open on weekends. The thing is a mess. Why would he go and report to his police station if they are going to turn him away? Is that common practice? Is that what should be happening?

Ian Dyson: In any call centre function, there will be a percentage of people who cannot get through—I will be absolutely candid about that. But let us look at this: Action Fraud operates 24/7. We moved to that in October of last year. It is, to our knowledge, the first and probably most comprehensive fraud and cyber-reporting capability anywhere in the world. Given that this is a crime type that is global in size and scale, that is really important, because the risk is that you would just get a very localised response that does not see the opportunities for the linkages of individual reports.

The response from that local force was not the correct response. As a result of some of the work we are doing—we are going around doing peer-to-peer reviews of forces, and we have done 26 to date—which is to help them understand how to improve their response, we want them first to identify vulnerability at that first point of report, to see if any immediate action can be taken. They are expected to do that. If not, they should take the report and report it to Action Fraud, sending it to us so that we get the comprehensive picture.

The example you described is not one that I would want to continue. With the Home Office, we are investing in a new system, which will be far more agile. It will have, for example, TrackMyCrime and a far more user-friendly and intuitive website. In the three years since we took over Action Fraud, we have shifted from 70% telephone reporting and 30% online to roughly 50% each now. We want to continue that channel shift so that we can provide a better service.

Q74 **Layla Moran:** Back to the scale of it, Mr Rutnam, when will you have better data on the costs of online fraud? We know that you make estimates, which we are working with right now, but what do you need in order to make this less of an estimate and more of a certainty?

Philip Rutnam: That is a really interesting and challenging question. I have only been in this role for six months, and I have been struck by the enormous range in estimates of the cost of fraud to the economy—between £10 billion and £144 billion—and very different methodologies as well as sources underlie those figures. I will pass this to Mr Riley, the senior official in the department directly responsible.

Richard Riley: You will have seen the work of the Joint Fraud Taskforce as five very clear work strands to address the problem. All of that is underpinned by a work strand about understanding the threat.

What do we know now? We have a level of certainty about the data and the instances of fraud that come out of police recorded crime. That is a start. Over and above that, we know what the indications of the crime survey for England and Wales tell us—so we have some further data. We have further data from industry surveys and the intelligence picture that Commissioner Dyson and the National Crime Agency are pulling together. All of that is giving us a developing picture of the scale and nature of the threat.

There are some big numbers here, but there are individuals—victims—on the end of it. I completely get that as an official, and other colleagues do as well. So however big it is, we think—genuinely—that we have some places to start on what the nature of the problem is now and what would make a strategic impact on it. Thus the work of the Joint Fraud Taskforce targeting those particular points.

Apologies for my voice, Chair.

Chair: The ghost has gone for now.

Richard Riley: I have Strepsils.

Q75 **Layla Moran:** Mr Rutnam, we heard from the banks that, for various reasons, they are reluctant to report their own figures about how much they are losing. How can they get away with it, in your opinion? How is it right that banks cannot report on how much fraud is happening?

Philip Rutnam: The question is probably specifically about whether the banks are reluctant to release their own individual information about an individual bank's performance.

Layla Moran: Indeed.

Philip Rutnam: The position at the moment is that there is not a legal requirement on them to report individually about the scale of fraud. There is very good industry co-operation, as I think you have heard. I think there are also very good signs of industry co-operation with Government. But there is not a requirement on them to disclose the level of fraud, for example, in their annual report and accounts or other piece of financial regulation.

At the moment, it is not the Government's policy that they should have to do that. Our policy, which we are working to and focusing on, is seeking to achieve results in the form of a significant reduction in the level of fraud over time, to deal with all the challenges we are talking about. We are seeking to achieve those results, most effectively by working first through voluntary means, the sort of partnership we have been hearing about.

Q76 **Layla Moran:** But if they are not reporting it, how do we know that is true?

Philip Rutnam: The banks do report frauds. They report very large amounts of information to law enforcement. That is information that we can access to produce—

Q77 **Layla Moran:** May I just clarify? It is not mandatory that they report this information; it is voluntary. Is that correct?

Philip Rutnam: Let's distinguish. First, it is not mandatory that they report individually, nor to the public in relation to the level of—

Q78 **Layla Moran:** I am talking specifically about a referral of an individual case to Action Fraud. Do they have to do that?

Philip Rutnam: No, that's not mandatory, either. However, there is a very strong expectation on them that they would do so.

Q79 **Chair:** Why is it a strong expectation? Why not mandatory? Why would they not do it?

Richard Riley: We heard an important point before about lessons from history. I wonder if I could give two from different periods.

Chair: Very quickly. Too much history takes us a long way down the track.

Richard Riley: I think it might be instructive. In 1992, the then Government published a car-theft index. You will remember that at the time there was distinct public and parliamentary concern about the level of car thefts. As a way of delivering changes into the system and getting the industry to take responsibility, which they then did, to target-harden cars, a car-theft index was published. That is one way of approaching the problem.

The second one I would give you is the introduction of chip and PIN, which has already been mentioned. Chip and PIN was introduced industry-wide after some trialling in 2006. That was not on the back of an index of the

worst card manufacturers or suppliers. It was an industry-Government level of co-operation. That is the approach, as the Permanent Secretary has said, that the Home Secretary has asked us to take: Joint Fraud Taskforce, co-operation, collaboration, with challenge in the system, not compulsion, at this stage.

Q80 **Layla Moran:** But wouldn't the league table help?

Richard Riley: Brian gave you an indication about one of the unintended consequences of that. One of the others from our perspective is—and I'll be honest—that the quality of the data that we would have for me to be able to advise Ministers to publish a table that looks like that, with the banks ranked, does not support that. The Government would presumably be open to quite significant legal challenge from the banks. Thus, the point about working hard at the data. Until we can do that, I don't think we will be in a position.

Q81 **Layla Moran:** So, you are not ruling it out for the future. You just have to improve the data.

Philip Rutnam: It is not the Government's policy now. That does not mean it is ruled out for ever. What we want to see, though, is results; we want to see outcomes.

I would make another point. Mr Dilley mentioned earlier one reason, in relation to fraudster behaviour, for being cautious about publishing bank or institution-specific data. Another key point is that many of the solutions that we think need to be put in place are actually industry-wide solutions. They are things that need co-operation across much or all of the relevant players in the industry, such as the move to deal with card-not-present fraud. That is really only likely to be delivered effectively if we have industry-wide co-operation.

Chair: I think Ms Keegan has quite useful experience and has a particular question on this point.

Gillian Keegan: You use the analogy of chip and PIN, which I was heavily involved in. The difference between then and now is that the fraud that was being experienced at that point and the forecast of growth in fraud was being borne by the banks. It was the banks that were losing out. In this case, one of my concerns, and perhaps why this action and activity are a bit more passive, is that it is about consumers. The risk has spread and it is not sitting with the organisations. They are not even getting reported. Whether it is the banks, the bank accounts, the technology that is servicing that or the payments technology, they are not the ones wearing the risk and the cost in many cases, and that will change the activity levels, and I think that is what we are seeing.

Q82 **Chair:** Do you think that is the case, Mr Riley?

Richard Riley: I think we recognise the point about the spread of risk, so we are working with the Joint Fraud Taskforce. We are concentrating on five areas—Ministers have agreed this—to make a strategic impact on the problem. I will point out two of those areas. One is card not present fraud,

as the permanent secretary said. That addresses the big bulk strategically of where the problem is now. That is why we are working with the industry on that. To the point on authorised push payments, that is why we have a whole strand of work on funds repatriation where we will be working with the banks to find technical and legal frameworks by which the banks themselves and law enforcement can work to address exactly the problem. We are addressing the problem that is manifesting itself now and a bit of the problem that Brian spoke about in terms of the future.

Q83 **Chair:** Can I just pick up on the legal framework before I go back to Ms Moran? Are you suggesting that new laws will be necessary to do this?

Richard Riley: In the work that we are doing on the funds repatriation point, we are looking at whether there is sufficient legal cover for the banks to repatriate funds to victims, where they can be identified. There are some questions.

Q84 **Chair:** So will there perhaps need to be new laws passed through this House?

Richard Riley: If there is a need for legislative change, we will be approaching the Home Secretary with an indication of what that might be.

Philip Rutnam: Can I just add that this is where the flow of funds is carried on through the banking system? It is where a bank has made a transfer to another bank. This question of unauthorised payments is where we think a funds repatriation solution could really—

Chair: That is a useful point to clarify before everyone thinks they are going to get their money back from every scam.

Philip Rutnam: Exactly.

Q85 **Layla Moran:** I totally take the point about fraudsters going after the weakest link in the chain—the weakest bank—but equally the purpose of this Committee is to champion the rights of the consumer, and there is a balance to be struck in holding them to account. Does UK Finance share the individual bank details with the joint taskforce? By that, I do not necessarily mean making it public so that fraudsters can get hold of it. Are you, Mr Rutnam, holding them to account for what they say they are going to do? Who is making sure that this is getting done?

Philip Rutnam: I am going to ask Mr Riley to answer.

Richard Riley: The short answer is that the Home Secretary chaired the latest iteration of the oversight board on 11 September, where she vigorously held MasterCard and other representatives of the private sector to account for delivering as quickly as possible a technical solution to card not present fraud.

Chair: Sorry, that is not at all an answer to Ms Moran's question. Would you like to repeat the question, Ms Moran?

Q86 **Layla Moran:** My question was about the individual bank's performances as a league table, or however else you wanted it to be presented. At the

moment, all the knowledge is being held by the industry. Who is holding the industry to account to ensure that what we have is a race to the top in terms of safety? I appreciate that it might not be something that you want to make public, but do you not think that it is your job—

Chair: Do you see that data?

Richard Riley: I don't see the data. I don't see the operational data; law enforcement colleagues will. I am a policy official; I am not an operational leader. It is the job of the Joint Fraud Taskforce and me, as chair of that board—

Q87 **Chair:** So you do not. Commissioner, what do you see?

Ian Dyson: I see some data, yes. What I think I don't know is what I don't know. I get data into the National Fraud Intelligence Bureau from the banks through Cifas. It is known fraud that they have shared within Cifas, and then we get—

Q88 **Chair:** So you get the known fraud, but for individual cases, do you get an aggregate number for which banks have got more of a certain type of fraud than other banks in a league table?

Ian Dyson: I do not have that data, no. I also get data through UK Finance.

Q89 **Chair:** Is that data anonymised?

Ian Dyson: It will be trend data. It will have details about suspects and so on.

Q90 **Chair:** So it has data on individuals and trends. Does it say that bank X has a bigger problem with card not present fraud than bank Y, which is doing a good job on it?

Ian Dyson: No. What it would provide me with is intelligence from which I can look at action to be taken for enforcement or prevention or protection.

Q91 **Chair:** So even you as the commissioner for the police force responsible for this issue do not get to see the detailed bank data, even though, to be clear for the record, you would treat that confidentially, would you not?

Ian Dyson: Correct.

Q92 **Chair:** If banks were to share that with you, it would be used for tackling this crime and for no other purpose and it would not be released to anyone.

Ian Dyson: That is correct.

Q93 **Layla Moran:** I think that what this line of questioning perhaps shows is: where does the buck stop? Who is ultimately responsible for all the recommendations that you may or may not accept in the NAO Report? Now that we are in 2016, if we have recently published long-term goals from the joint taskforce, where does that buck stop? Is it with you, Mr Rutnam, or the Home Secretary?

Philip Rutnam: I think I have already tried to answer that question in describing the Home Office's role, as we see it, as providing strategic leadership for the country in responding to the problem.

Q94 **Layla Moran:** Surely that is just a yes or no question.

Philip Rutnam: I was going to go on to add a little supplementary to that. What we have sought to do—what, in fact, we have done—is to turn that question of how you provide strategic leadership, into a series of actions that could actually make real difference to the problem. On dealing with card not present fraud, we have said that we want to see a very significant reduction in CNP fraud by 2019. That depends on action by the banks, and we will hold the banks to account in a constructive way for delivery on that. Similarly, coming up with a solution on funds repatriation, going back to the earlier point about unauthorised payments, would provide a very significant step forward in dealing with that. We have turned the question of providing strategic leadership into a series of big tasks for which we will hold individual sectors or organisations to account.

Q95 **Layla Moran:** But if they do not deliver, what happens then?

Philip Rutnam: We have already described our focus on results, outcomes, making a difference—

Q96 **Caroline Flint:** I do not understand how you can talk about outcomes making a difference if you have not got a sense of what the problem is. You have a situation, as has already been raised by yourselves and other witnesses, about where people go. If someone finds they are losing money, they are initially going to go to their bank. Before anybody else, they are going to go to who is holding the purse. If the banks are not saying to them, "By the way, you better report this to the police," or passing that on to the police, you are basically being carved out of a huge amount of data that can help inform you about different types of fraud and how it is working. So tell me, Mr Rutnam, how can you be strategic and how can you deliver when you do not know the extent of the problems and where the weaknesses or the peaks in certain types of fraud are appearing?

Philip Rutnam: I think we do now have a pretty good sense of the scale of the problem. We now have national statistics, which are the first of their kind in the world, showing that there were over 3 million frauds in the last recorded year, of which just under 2 million were online fraud. How will I tell by 2020 whether or not we have made a difference? Is that number the same? Has it gone up? Has it gone down? That is a very high-level measure, of course. We continue to need to improve the evidence base, for all the reasons Mr Riley has identified, but we do now have some kind of baseline against which we can measure progress, and doing the things that we have—

Q97 **Caroline Flint:** What if the way you gather and collect the information at baseline is completely distorted, and you are therefore, I suggest, in a sense of false security about what the final outcome will be? Those net figures do not necessarily reveal the types of fraud or where the weakest

points in that chain are, let alone being an accurate baseline figure.

Philip Rutnam: I do actually think the statistics that have been published will provide a good baseline—not a perfect one, but a good one, I hope. Those statistics were published by the ONS. Its approach to developing those statistics in this area began in 2010, it launched a major project on this in 2012 and a significant amount of work has gone into developing these statistics under the guidance of the national statistician. We now have a statistical evidence base, which should tell us in future years whether online fraud is going up, going down or staying constant. That will be a very important metric for us.

Q98 **Layla Moran:** But that is based on the 20% of self-reported crimes, which therefore means it is a biased sample. How can you be sure that you have an entirely unbiased sample unless you have mandatory reporting at key points in the system?

Philip Rutnam: That isn't actually how that statistic is assembled. That statistic comes from the crime survey for England and Wales, which is based on a very large survey of households—something like 50,000—in order to assess their experience of crime. It is overall the best guide that we have to crime and crime trends. It is not perfect, there are some omissions from it, but it is not the 20% self-reported—

Q99 **Chair:** But, Mr Rutnam—and, in fact, Commissioner Dyson—you spoke earlier about the reporting rate of 250,000 a year, which given the scale is a very tiny proportion. Is it a problem of communication or capacity? You said it is a 24/7 service for online fraud. People can report it in, but they aren't, are they? As Ms Moran says, without the data, how do we know we are making an improvement? Is it capacity or communication?

Ian Dyson: I think it is a combination of both.

Q100 **Chair:** You highlighted some of the reasons why people are embarrassed, and so on, but do you think there are issues to do with the system, rather than the individual reporting in?

Ian Dyson: As more and more of our business is done online, we are seeing that fraudsters have greater opportunities to commit fraud. We need to invest our time in prevention and the education of the public.

Q101 **Chair:** But people are not reporting it. Why is that? Are you happy with that number?

Ian Dyson: No, I am not happy at all. I think there are some constraints around the current reporting system, which I outlined.

Chair: I think Ms Moran did some mystery shopping, which threw up some problems.

Q102 **Layla Moran:** I did indeed. In fact, it was on behalf of the gentleman who contacted me about the Microsoft scam. I went online and tried to get in contact. There was a number, but it was made very clear that it was only for organisations. The only way I could talk to someone was on an online chat, which I imagine is an alien concept for some people. I then went on

to the online chat and asked whether there was a number I could call, and I was told that, yes, I could. In fact, it was the number that was advertised, but they purposefully do not advertise when anyone can call it. I asked specifically, "Do you advertise when people can call?" and the answer was, "No, we do not advertise."

How are we going to encourage people? Earlier, you said that people are shifting to reporting online, rather than reporting on the phone. Don't you think that is because they are told they can't call in? That's why there has been a move—they just don't report it at all.

Ian Dyson: I will need to confirm that.

Layla Moran: I've got the transcript of the chat here.

Chair: We can provide you with all the documents.

Ian Dyson: I would be interested to see that. The headline for me is that Action Fraud is available 24/7, both for telephone reporting and online. You asked whether the shift is because people are fed up of reporting online or are being discouraged from reporting by telephone, but actually if you look at a lot of other industries, people are shifting their business online. We want to create the appropriate environment. Whether you wish to call by telephone or whether you wish to go online, we can provide that service.

Yes, there are systemic constraints at the moment. The new system we will have online very soon will enable a much more fluid, user-friendly approach to that. The reality is that all call centres provide services based on the resources they have. That is one constraint.

There are those factors, which I described earlier, about why people may choose not to report. I referenced the earlier conversation about the banks. Yes, people who experience fraud from their bank account will go to their bank first. We are talking with the banks about the prospect of them having a facility that they can immediately refer straight into Action Fraud, so they do not just advise people to report. That is a one-stop service.

Q103 **Layla Moran:** Could you give an estimate of the proportion of banking transactions that are reported to Action Fraud? Do you know, roughly?

Ian Dyson: I don't have those figures to hand. Of the 500,000 reports we get a year, roughly half are received through Action Fraud reporting by individuals, and a similar figure comes from the data we get from UK Finance and Cifas. That enables us to—

Q104 **Chair:** Do you think that is the right proportion? I mean, the banks must be dealing with a lot more people than the individuals who consider hopping online.

Ian Dyson: UK Finance would say that they prevent, with the systems they have built in their banks, about £7 out of £10-worth of fraud—for every £10-worth of fraud, they reckon they prevent £7. Having seen the banks in action, I think they have invested significant sums in prevention

methods, and I welcome the opportunity to work more with them. The challenges with data sharing were discussed with the Permanent Secretary earlier. We constantly work to try to improve that. Certainly, for example, we have tried and established methods with the banks requesting data or information on bank accounts that we wish to investigate. I am not sure we quite geared that up for a global and big-data—

Q105 **Layla Moran:** But if you had access to full individual reporting figures and could compare that with those you have got, surely that would give you a pretty accurate view of how much of it is actually getting through to you.

Ian Dyson: Yes, it would.

Q106 **Chris Evans:** I have a few quick questions for Mr Rutnam. You will know of copycat websites masquerading as Government websites: everything from car tax and passports to congestion charges and registering a bereavement. I had a Westminster Hall debate about this in 2014 and the Minister at the time said that the Government was stamping it out. It is still a major problem. There are people online at the moment talking about ordering European health cards, which can speed up the system. What is the Government doing about these? Because these are essential services.

Philip Rutnam: You are right that this is a material—a significant problem. I know of cases myself, as well, personally. I would relate this challenge to the Government's wider national cyber-security programme which was launched last year—of course there was a cyber-security programme before that—with a very significant increase in the level of resource put into it. It includes the establishment of the landmark National Cyber Security Centre: a centre of expertise bringing together, again, Government, access to private sector, access ultimately to specialist resources deep inside law enforcement.

One thing that is being taken forward in the national cyber-security programme is what is known as active cyber-defence, which includes methods of checking whether or not a website is genuine and methods of resisting fake emails which claim to come from a gov.uk website. So there is a whole strand of activity. In fact, the First Secretary of State, who oversees the national cyber-security programme, is making a speech today on this programme. Richard oversees our involvement in the Home Office and may want to add something.

Richard Riley: I want to add to that the work of the National Crime Agency in conjunction with the National Cyber Security Centre, so you get the protection but you also get the investigation. The National Crime Agency is explicitly set up to include cybercrime within their remit to look at the investigation about the perpetrators behind exactly the scams—

Q107 **Chris Evans:** The huge problem I came across when I looked into this subject in depth was that no one knew who to complain to. There is no point in complaining to the website owner because they will not respond. I would advise some people to complain to the Advertising Standards Authority, local trading standards or the Competition and Markets

Authority. There were numbers of areas and different people would give different advice. If somebody is a victim of a scam where they have tried to pay the congestion charge and somebody has creamed off £2, who would you say they should go to? What is the official advice?

Philip Rutnam: This is a type of fraud. If they contact their local police force, they will be referred—I expect—to Action Fraud. One of the reasons why we need to improve Action Fraud—to significantly improve the way in which it interacts with the public and business—is to make it easier to report this kind of crime. So Action Fraud is the place to go.

Q108 **Chris Evans:** How many websites are you shutting down every week on this? At one point there were about six of these popping up when I was looking at this.

Philip Rutnam: I am afraid I do not have a figure for that. There is a very—

Q109 **Chris Evans:** But we are still shutting them down once they are discovered?

Philip Rutnam: I believe so. The commissioner may be able to speak on that. There is a very significant volume of what are known as disruptions, which come out of things that are reported to Action Fraud that go into the National Fraud Intelligence Bureau that sits behind Action Fraud. I think they undertake over 100,000 disruptions a year of various kinds.

Ian Dyson: Yes, that is correct. In an average year we will disrupt and close down about 180,000 a year. This figure includes bank accounts, websites and telephone lines that are associated with known fraud. In respect of your particular issue, yes, there are frauds that sit behind some of them. They are not all frauds. If somebody advertises that they will get you a visa to travel to the US through the US embassy, you get a price and they do it for you at a fee, and you receive the visa, that is the challenge. If you don't get a visa, then there is a fraud involved, but if they do provide that service and you've paid—

Q110 **Chris Evans:** That is where the grey area is. If that happens to you, who do you complain to? You might go to the police and they ask whether you have received the visa, and you say, "Yes I have". Or it might be the European health card, which is free, but there are people charging 20 or 30 quid for it. Where do they go from there? If someone says they have been a victim of fraud, and what they have been a victim of is false advertising, who would you send them to? That is clearly going to be a problem.

Ian Dyson: We have good links with trading standards and we would refer them to talk to trading standards.

Q111 **Chair:** That is interesting. We could have a look at trading standards, although it is a local authority issue. I am sure you would agree that there are big variations even between London boroughs about how much money is invested in trading standards.

Ian Dyson: Yes.

Q112 **Geoffrey Clifton-Brown:** Reading the NAO Report, I get the impression that you and your force is doing a good job, but there would seem to be very few other exemplar forces among the rest of the 42 forces, although Sussex is specifically cited. What is being done by your force as the lead force to disseminate best practice among the 42?

Ian Dyson: Policing is local and locally accountable, so the decisions on what a force will prioritise or consider to take action against is a matter that is locally accountable by the chief constable to the local police and crime commissioner. They are balancing the referrals that I send to them against all their other areas of vulnerability, including public protection, modern slavery and domestic abuse. So we have to work in that sort of landscape, where it is very much a local policing service.

Having said that, we have and we are looking to work with forces. While it is true that the number that have fraud as a priority in their local policing plan was very low, 41 of the 43 forces have vulnerability and protecting vulnerable victims as a priority. That can include all sorts of different crime types; the victims are still very similar.

We send out twice a year an infographic to each chief constable and each police and crime commissioner, which sets out very clearly what fraud has taken place and been reported to us that occurred in their force area, the breakdown of victims, the number of disseminations and intelligence and reports that we have sent to them in that year, and then their return rate in terms of outcomes. So it is very publicly available, and they can see what the performance of the local force is.

We have also done peer reviews to assure ourselves and to look at how forces are dealing with fraud in their local area and giving advice based on our expertise. We have done 27 since June of last year and that is an ongoing programme. You may be aware that HMIC will be inspecting on fraud later this year or early next year. That is to get them to a good standard. I am pleased to say that 35 of the 43 forces have a degree of local fraud capability within them now, which is an improvement on what we saw three or four years ago. The ones that do not have relationships and linkages into the local and regional organised crime units, which have a fraud team.

We also send out advice. We sent out 800 separate pieces of advice to forces on prevention and protection, which they can disseminate through their networks and community groups. We have best practice guides. We have worked with the College of Policing on training, so that fraud is a specific element of the national investigators programme. We have a national responsibility for training—we have an Economic Crime Academy. I have trained officers from 25 forces since March of this year.

There are a whole range of things that I am doing, given that I cannot mandate to any other chief constable.

Q113 **Geoffrey Clifton-Brown:** Can I ask you about prosecutions? Can you give us any figures on prosecutions? Given the rise and the scale of this crime, we would expect a rise in prosecutions too.

Ian Dyson: The CPS reports that it has a 30% increase in the number of prosecutions for fraud and bribery over the last 18 months, I believe, but that is CPS data. In terms of our data, the number of prosecutions has actually dropped slightly. I have looked at the reasons behind that, bearing in mind that some cases can go on for years and that there is never a direct cause and effect of whether a court proceeding in one year will lead to a judicial outcome in another. But what I can say is that of the 240,000 crime reports, we disseminated to police forces for further action about half of them—about 127,000.

That does not necessarily require an investigation per se. I go back to the fact that we are really emphasising the protection and prevention aspects in relation to this crime type, so it might be for additional support for vulnerable victims and so on. Of those 127,000, 70,000 were cases that we assessed as having a viable investigative lead that the forces could investigate. That goes into their local assessments and their local prioritisation task and co-ordination.

There are outcomes both judicial and non-judicial from cases now. What we have seen over the last three years, on average, is that we have an outcome being recorded against 45% of those disseminations that we send out, and 13% of the crime reports that we send out. In terms of judicial detections, which I guess are at the heart of your question, 14% of the cases we send out for action have resulted in a judicial outcome to date.

Compared with the total volume of crime, that is of course very low, but I would argue that what we are doing here, with a national lead force, is probably what we are not doing with a lot of other crime types, which is trying to focus our capability, our investigative resource, on those cases that have the best chance of getting a judicial outcome. The others—those 118,000—we use as intelligence to help to prevent and protect.

Chair: Thank you for that comprehensive answer. Mr Clifton-Brown now has another important meeting to attend.

Q114 **Martyn Day:** Mr Rutnam, you mentioned the cyber-security strategy. Earlier this year, just before the summer, I got a parliamentary answer from the Cabinet Office that highlighted the fact that the gap between the supply and the demand for cyber-security experts was estimated to reach more than 40,000 by 2020. That is without intervention; obviously, there will be intervention, so it is not going to be the worst case. Do you think that estimate is realistic, and what steps are you taking to ensure that the Joint Fraud Taskforce and Action Fraud get their share of the cyber-security experts?

Philip Rutnam: I cannot really comment directly on the estimate, because the national cyber-security programme sits under the Cabinet Office rather than the Home Office, although we have a significant role. My personal view is that it sounds about right. The proposition that there would be a significant gap—a large skills need—sounds absolutely right. In terms of what we are doing, I see it as principally the responsibility of each of the sectors involved—the banking and finance sector, the law

enforcement sector and Government—to make sure that they have a skills strategy that will address their business needs. We will be working particularly closely, of course, with the law enforcement sector, which we support in a number of ways, to make sure that they are able to skill themselves up. Again, Richard might be able to speak in more detail.

Richard Riley: Mr Day, in terms of the share that is coming to the Home Office on fraud, there is £1.9 billion of Government money over the spending review period, as part of the national cyber-security programme. This year, 2017-18, the Home Office share of that on cybercrime is £31.5 million, and we have been working very closely with law enforcement colleagues on the distribution of that money. The majority of the money is supporting national and regional endeavours, with some additional funds for the City of London police and the Metropolitan police. So this year it is £31.5 million, predominantly regionally and nationally based, to address the capability gap—one of the gaps that you have described.

Philip Rutnam: The commissioner could perhaps add something from his perspective.

Ian Dyson: Mr Day, we work very closely with the National Cyber Security Centre. They have a programme they are developing of scholarships for both graduates and sixth-formers on cyber-skills. We are engaged with that programme and want to be part of receiving the benefit of some of those.

The other point I would make is that I have very good relationships with lots of different industries. At any one time I have probably about 20 to 25 people on secondment from industry, giving me skills that I would perhaps struggle to recruit into the public sector.

Q115 **Martyn Day:** That is where I was going next. The Report highlighted the fact that as few as one in 150 police officers was engaged directly with online fraud. It is so specialist that maybe police officers are not the key people on many occasions. Do you feel that you have enough specialist support?

Ian Dyson: Any investigation requires a degree of investigative experience, so there will always be a case for detectives in this world. I referred earlier to the fact that we developed, with the College of Policing, specific training on fraud and online investigation. Blended with that is that I have a significant number of police staff who are not warranted police officers and who do a lot of my analytical and data-crunching work and so on, and I supplement those with secondments from industry.

If I could just give one very quick recent example, one of the big frauds that we are dealing with at the moment is the computer software fraud in which people ring up and say they are from Microsoft and then get on to your computer. We made six arrests in the UK earlier this year. We were receiving into Action Fraud about 2,500 reports a month on computer software fraud. Since those arrests—we believe that was the key network operating in India and the UK—those reports have dropped to 1,000 a month. It had a significant impact, and that is a really good example.

Q116 **Chair:** Are you affected by the issue about headcount of warranted officers? I do not know if it affects City of London police the same way as it affects the Met. Some borough commanders say they would prefer to have more analysts and warranted officers; they don't quite put it that way, but they recognise the benefit of analysts in tackling crime. Putting all the money into warranted officers can mean you lose analysts, who are important. Is that something that affects City of London police?

Ian Dyson: It can affect us. We are slightly different in scale from the Met.

Q117 **Chair:** Do you have a headcount number for warranted officers that you have to achieve?

Ian Dyson: I do not have a particular limit, but in my national lead force work I have 75 warranted officers and something like 58 non-warranted officers.

Q118 **Chair:** Do you have to keep that balance, or is that your judgment?

Ian Dyson: That is my judgment, and then, for the broader force, I have a broader responsibility.

Chair: Okay. That's fine, thank you.

Q119 **Martyn Day:** Moving on slightly, from a policing perspective, you are obviously all involved in the taskforce. Who else do you feel should be added into the taskforce that would help with the greater pool of information and data sharing?

Ian Dyson: There are a number; I have shared with the Home Office other Departments and agencies that could be involved. I know the Home Office is expanding the remit of the taskforce. From my point of view, the retail sector is coming into it is great news. I think there could be great opportunities for representatives from the telecommunications industry. The other one that we see as a big enabler of fraud is some of the professional enablers, as we call them—the fraudulent solicitors and doctors who generate a lot of fraud. Some of the regulators around the professions could be a useful addition to the taskforce.

Q120 **Luke Graham:** To follow up a little bit with Commissioner Dyson on the sharing of best practice—it is great to hear that you are sharing the infographics—I just want to understand what part technological advancements are playing in sharing that best practice? I ask the same question to Mr Riley but from a different side: how big a part are technological advancements such as blockchain playing, and how much are you engaging with industry and other partners to develop that technology and pass it around our police forces, retailers and banks?

Ian Dyson: Technology is an important part of this, and I think it is also the solution to a lot of it; you talked about card not present earlier. Frankly, I think we in law enforcement are still trying to understand some of the impacts of crypto-currencies and blockchain. We are doing that work at the moment. It is certainly allowing the whole landscape to be

more fluid, agile and perhaps, sometimes, slightly more challenging, in terms of jurisdiction.

On the best practice that we are developing and sending out to forces, we probably should not get too drawn down the road that all fraud is cyber-enabled. There is a significant amount of fraud that is still conducted on the telephone. In fact, the email—a quick email; not huge technical ones, but a scam one—is the biggest single route that a fraudster will use. Actually, some of the best practice that we can send out to forces is about how they can advise people on what I would call email hygiene and those sort of things.

In terms of how we are engaging with the industry around the bigger things, I will perhaps leave Mr Riley to comment on where the Home Office is on that.

Richard Riley: We are talking just for the financial sector through the Joint Fraud Taskforce. As the commissioner said, we are expanding its membership out to the retail sector and the big online retailers as well. Part of that is that Ministers are asking us to develop a constructive relationship with industry, so that when it is developing new technological developments for its own purposes, we are able to have a conversation about where those developments could be exploited by criminals. As we found, and as the commissioner knows, the criminals are rather good at exploiting weak links in the system. Candidly, they are perhaps somewhat better than us policy officials. At the very earliest stages of the development of new technology, can we design out crime opportunities and design in protection right from the start? That is the kind of conversation we are having with industry now as part of the Joint Fraud Taskforce.

Q121 **Chair:** Akin to the fact that people cannot break into cars quite so easily now because of smart keys.

Richard Riley: Yes, that is one of the lessons. The crime stats are stark around car crime. It is a lesson, but the context is very different.

Chair: We can still do that in the tech world, as I know from Shoreditch.

Q122 **Luke Graham:** Mr Riley, you are working with some of the big retailers and institutional players. As Mr Dyson said, it is a dynamic and fast-moving sector. Do you have any specific initiatives to engage with the more entrepreneurial firms? We have Shoreditch and we have the City; we have some leading financial tech hubs in London specifically. Will there be specific initiatives to engage with the smaller players as well, to feed back some of their dynamism and bring in some of their innovative thinking to try to get ahead of the curve, rather than chasing it?

Richard Riley: Specifically on fraud, we have been talking to some of the challenger banks, because they are in a very different position from Brian's organisation. If I am honest, the centre of gravity on discussing with Shoreditch and all the rest of it is through the National Cyber Security Centre. The experts at the NCSC are the people who have been engaging

with the kind of entrepreneurs that you are talking about, Mr Graham. They have been talking about cyber-security writ large. The Government's ambition, as the Home Secretary has said, is to make the UK the best place in the world to do our commerce online. London has got to be a safe and brilliant place to do financial work, but it has to be safe from cyber-attacks. The National Cyber Security Centre is where the centre of gravity lies.

Q123 **Martyn Day:** What assurances can you give us regarding the permanency or otherwise of the taskforce?

Philip Rutnam: The taskforce does not have an end date. The taskforce is a strategic partnership that I expect to have a long-term future—a future that is counted in a number of years. We will obviously want to ensure that it is delivering what we expect of it, but I have every reason to hope that with the right effort and the right will, it will deliver the right results.

Richard Riley: We used the word "taskforce" at the start because it was trying to initiate some momentum into the system, but Ministers and industry have been clear that long-term sustainable reductions in fraud require long-term sustainable investment from Government, law enforcement and industry. That is what we are after.

Q124 **Martyn Day:** Can you give us some examples of what teeth it has? How can it get the data that seem to be missing in the system? How can we ensure that money that is collected goes back to the people who have been defrauded?

Richard Riley: In terms of the taskforce itself?

Martyn Day: Yes.

Richard Riley: I suppose—I know you did not like this answer last time—there is the fact that Ministers, the Home Secretary, the Economic Secretary to the Treasury and the Security Minister call together CEOs and senior people from the banks to look at the progress we are making under the auspices of the Joint Fraud Taskforce and say, "It is either good enough or it is not. If it is not, what consequences flow from that?" There is pressure into the system from Ministers and from us working collaboratively with industry.

Q125 **Martyn Day:** As the Chinese say, we live in interesting times. Clearly, you have many other competing priorities. How do we guarantee that this issue stays at the top of the agenda and is not sidelined by issues such as Brexit and the terrorism situation?

Philip Rutnam: This is a very high priority for the Home Office, because the whole mission of the organisation is to protect the public. This is now the most common type of crime. As I was trying to explain earlier, it is a matter of not just financial losses but a real impact emotionally on hundreds of thousands of people, which is tangible through stories that we hear directly when we meet them, and strategically, on the reputation of our financial system and our economy and the confidence that people

have in the ability to do business online. All the drivers for paying very close attention to this issue are there, and I do not see them going away—not until we have really made of lot of progress in dealing with the issue.

Q126 **Gareth Snell:** I am not sure whether this is a question for Mr Rutnam or Mr Dyson. A number of colleagues around the table have tried to pin you down this afternoon on who is ultimately responsible for this. You have talked about long-term funding arrangements and requirements. Can you confirm whether you have those funding commitments in place?

If we put aside the concerns that the Committee has expressed about the validity of the baseline of your statistics, because of the mechanism by which you have compiled them, what would have to be the reduction in fraud and over what period for all this work to be considered successful? If that target over that timescale is not met, who is ultimately accountable?

Philip Rutnam: We have not set formal targets yet.

Q127 **Gareth Snell:** When will that happen?

Philip Rutnam: Perhaps I should rephrase that. We have not set formal targets.

Gareth Snell: That is not rephrasing. Those are the same words you said in the same order.

Chair: "Yet" suggests you are going to, Mr Rutnam—a slip of the tongue there.

Philip Rutnam: It is obviously a matter for the Committee to conclude what it concludes, but one can see a natural progression in this. We have got the enterprise of the taskforce up and running, having got some momentum behind it. As the NAO said in its Report, we need to put some more formality and structure around it, which we are doing. The point about having a baseline against which one can measure progress is that then you can measure your progress. It will obviously be a matter for Ministers whether we set targets or not, but I want to reassure you about the scale of the ambition. Indeed, the Home Secretary was talking to the Home Affairs Committee yesterday about the scale of ambition she felt there was in this area.

Q128 **Gareth Snell:** So would you consider a 1% reduction in 20 years a success?

Philip Rutnam: Instinctively, no.

Gareth Snell: So if you know what is not a success, at some point you must know what is a success.

Q129 **Chair:** Give us a range of what would be a success.

Philip Rutnam: Richard mentioned the example of car crime. I think there was a 60% reduction in vehicle-related crime after new standards were introduced by the manufacturers. I am not saying that that is what we will achieve in this case, but the point about a focus on prevention and

protection is that you get upstream of the problem. You need to do that at scale. Another example was chip and PIN, where, again, there was a very significant reduction. We are looking for some very significant reduction.

Q130 **Chair:** Those two examples have been repeated often this afternoon. I think what Mr Snell is quite rightly driving at is how you will know when you have achieved success, given that this is a moving target and that it will almost certainly be a growing area, because more and more transactions take place online.

Q131 **Gareth Snell:** And if that is not achieved, who is ultimately responsible? That has been asked by a number of us. Where does the buck stop? If we do not see a tangible reduction over an acceptable period, who is ultimately responsible for that having not happened?

Philip Rutnam: First, we are not yet in a position of putting a figure on what success looks like, but the direction—

Q132 **Gareth Snell:** What does failure look like?

Philip Rutnam: I am not going to go down that route.

Q133 **Chair:** We may push you on that. What about where the buck stops? The Home Secretary chairs the taskforce.

Philip Rutnam: The direction and ambition is clear. I have already said that I think the Home Office is in the position of providing national leadership on this issue.

Q134 **Chair:** So is it the Home Secretary, or you?

Philip Rutnam: We are responsible as officials for making sure that policy is effectively implemented. It is a matter for Ministers to set policy, including priorities and allocation of resources, but the level of ambition that the Government have in this area is high. If we do not achieve a reduction of the scale we are talking about, we would want to understand why that was the case.

Q135 **Chair:** You say the level of ambition is high. Mr Snell has pushed you. It is difficult to pull an exact figure out, but you have not even given us a range of what you see success looking like. It does feel a bit, as Ms Flint and I have highlighted, as though we have been over this ground before. In 10 years' time, what would you hope to be the case? Would this be a lower area of crime, like car crime?

Philip Rutnam: I am not going to give you a figure. I have given some examples of good policy changes that were made in the past that had a real impact on the level of crime. Before I even gave a range, I would want to do more reflection on, and some analysis of, what will actually be plausible, and under what conditions.

If it did not work, it would be important to reflect on why. One significant point is that we know which sorts of crimes are happening now—at least, I think there is quite a lot of understanding of what is underpinning those crimes—but this is a dynamic area. It is quite likely that new crime types in relation to fraud will come along as well, so it is important that we have

a partnership that is resilient and adaptive as the nature of the threat changes.

Q136 **Gareth Snell:** I take issue with a number of points that you have raised, but that might be for a different time. I understand that targets are not necessarily always helpful, but it is very important to give a range. If you are not willing to set a target, how can you be confident that the work you are doing now is the work that you should be doing?

You have just said that before you made a target or gave an end point, you would want to do more reflection and more research. If that is the case, how can you be confident that the work that you are doing now is actually having an impact in the right way on reducing the level of online fraud? Public money is being spent now to try to achieve something that you are not willing to quantify as being the right way of reducing online fraud.

Philip Rutnam: There are two things in particular that we prioritised with the banking sector and the financial institutions: one is dealing with card not present; the other is dealing with funds repatriation. We have prioritised those because there are 3.4 million frauds of which just under 2 million are online frauds, and of those 2 million, the bulk—well over 1 million; 1.5 million or something like that—are card not present frauds. The reason for prioritising that is that it is clearly a very large proportion of the whole problem. I could give a reason in relation to funds repatriation, if you like

Q137 **Gareth Snell:** No, that is fine. Let's work with card not present fraud as a discrete area. Given the work that is going on now, what would you expect to be the impact on the amount of card not present fraud that takes place over the next 18 months to two years?

Philip Rutnam: The honest answer to that at the moment, unless Richard wants to add something, is we do not know, because it will depend on the solutions that are arrived at in relation to card not present fraud. There are a range of technological solutions—an area where we need the expertise of the financial sector. There is also the question of consumer behaviour. The solution that needs to be arrived at is one that feels sufficiently intuitive and easy for consumers that they use it. That work is under way, but it has not finished yet—Richard has more expertise on that.

Chair: We will not go into that any further, because I need to bring Ms Moran back in.

Q138 **Layla Moran:** Something very concrete that you are doing to help solve this problem is the Take Five campaign. I have to tell you, in my preparation for today I have read through that many, many times and it's not very pithy, is it? How did the Government come up with those five points? I do not mind who answers that first, because I actually do not know who created it.

Chair: Mr Riley, take responsibility for Take Five.

Richard Riley: I will take Take Five. I am not quite sure what the five points are.

Q139 **Layla Moran:** That is the point. It is a public awareness campaign and no one seems to know what the five points are.

Chair: Is it perhaps the pithy, "My money? My info? I don't think so."? I have learned that bit.

Richard Riley: Take Five was an industry-led campaign at the start. As you say, it has not just been going for two weeks. The genesis of the Take Five campaign was: take five minutes, and pause before you authorise the payment of £10,000 to someone whom you barely know, or whatever it might be. That was an industry-led campaign, 18 months ago. "Take five minutes" was the genesis of the campaign.

Ministers asked us to have a look at how a new comms campaign to get into the prevention space would look. We worked very closely with FFA UK, as it was at the time, and the banks to do some analysis of that, including some qualitative analysis. We have moved the campaign on. It is now a joint campaign between us and industry, where we have evolved the campaign into what you see now, which is effectively, "My money, my info, no, I won't," using the hand, which you have seen, as a kind of device. That is where Take Five came from. We now have £3.3 million invested in the campaign, which will run until March.

Q140 **Chair:** We have different figures here. I wonder whether the NAO can just clarify the figure. We have £3.8 million from industry, and you just said—

Linda Mills: That is a joint-funded total.

Q141 **Chair:** So the £3.8 million was the joint funding?

Linda Mills: By Government and industry; that's right.

Q142 **Chair:** How much did Government put in? How much was directly from taxpayers?

Richard Riley: We are putting in £500,000. We have an evaluation programme around it with the industry. What does success look like? To go to Mr Snell's conversation about this, success is measurable improvements in behaviour, with people being confident enough to say no and to challenge when fraudsters are after their money.

Q143 **Layla Moran:** Would it be fair to say that a lot of these points centre on what is often the weakest link in security measures—the human, and their divulgence of their own habits and behaviour? Linked to that, we have heard suggestions from the Home Office that it wants to create a back door to the encryption services of things such as WhatsApp. Wouldn't that inadvertently make consumers more vulnerable to hackers getting that information?

Philip Rutnam: The short answer is no. The Government support strong encryption. There are particular issues around relatively few applications, which are based on something called end-to-end encryption. That is only

one subset of the types of encryption that are out there, and as far as we can see it is not necessary in order to achieve the level of customer security that is needed for transactions. What the Government want is to have a dialogue with the industry, and with relevant experts on both sides, about some of the business reasons and factors underpinning particular choices of encryption strategy. I would distinguish the encryption debate, which is a live debate, from the question of online security.

Q144 **Layla Moran:** But to bring you back to WhatsApp, I have a family WhatsApp, and I am sure other people in the room do as well. We know that while we give great advice about passwords being 10 figures long and having all sorts of exclamation points and whatever in them, a lot of people just use their dog's name. If someone was able to get into your family WhatsApp and find out what that was, would it not inadvertently make you more vulnerable to this kind of crime?

Philip Rutnam: Our advice would be that you can have very strong protection and encryption without it needing to be end-to-end encryption of the type you have mentioned.

Q145 **Martyn Day:** Mr Rutnam, at the start of today's session you mentioned the importance of national leadership, something I think we would all agree with on this matter. Last year, Which? had a campaign to try to get the banks to take responsibility for the push payment scams. Do you agree with that? Should we put more responsibility on the banks as a way of forcing them to create better protections for the consumer?

Philip Rutnam: Which? made a super-complaint to the Payment Systems Regulator, which the Payment Systems Regulator considered in line with its duties and the criteria that it applied. The Payment Systems Regulator came up with a range of recommendations, which should make a material difference to the situation on unauthorised payments. But at this point I would refer to the second major initiative that we are taking forward with the banks. We have talked about card not present. The other issue is funds repatriation, and a system of funds repatriation where we think there is a realistic prospect of developing both the technological and—subject to further consideration—the legal underpinning needed. A much better system of funds repatriation could potentially deal with quite a significant proportion of authorised payments.

It would not deal with all payments, because there will still be cases where people have taken money out of the bank and handed it to a rogue trader in cash, but where the payment moves on within the banking system, a system of funds repatriation that uses the best technology available to spot what are known as mule accounts and to repatriate money quickly could provide a lot of consumer protection. Mr Riley should add to that.

Richard Riley: I mentioned this previously. The funds repatriation work is explicitly mentioned by PSR as part of their response to the Which? super-complaint. They have recognised the work that the Joint Fraud Taskforce, again in collaboration with the banks, is doing on funds repatriation. As the Permanent Secretary said, there are some technical challenges here, and there are potentially some legal challenges, but the prize is a really

good one. This is about how you can track money back through the system that goes through multiple mule accounts, identify it, freeze it and return it to the victim, and, as a result of that, improve the intelligence base about what the mule account network looks like to be able to better assist law enforcement. The funds repatriation work is really important. It is one of the aspects of the response to the PSR's judgment on the Which? super-complaint.

Q146 **Martyn Day:** Thank you very much for that. What is your estimate of the timescale for getting funds repatriation up and running and delivering for people?

Richard Riley: We are doing this in a phased approach with the banks. A piloting phase is just completing around about now. We want to look at what the evidence from that piloting—that is the technical phrase—looks like before the end of the year. We will then go into another phase of testing. This is potentially tied up with the question about the legal framework, so we might have a technical solution but we need to work through the legal protection that the banks are asking for. Again, there is a bit of a lead-in time, because this is a complete systems change. I guess it depends when we have a legislative opportunity, but I would have thought it will be a couple of years before we have a fully fledged programme. What we will be pressing the banks to do is to see whether there are some classically quick wins we can do well before that to demonstrate the proof of concept.

Q147 **Chair:** I appreciate your honesty about the timetable. Rarely do we get a commitment quite so firm. Let's hope it's quicker.

I just want to come in on a couple of points. Picking up on Ms Moran's point about social media, Which?, in one of its excellent bits of work, has highlighted the issue of Facebook quizzes and so on. Commissioner Dyson, is this something that comes under your remit? Do you get lots of complaints about people using social media to get data and take over people's accounts and then use them in various ways to scam people?

Ian Dyson: The straight answer is yes, we do. There is no doubt that social media does play a significant role in a number of ways in fraudsters committing fraud. I would say this is probably where young people are more vulnerable than people of my generation, because they have a very different approach to personal information than we would. We have seen examples where young people have posted pictures of their newly acquired driving licence or passport online. Those are the sorts of things where we want to educate people, through schools and so on, that they need to take care. Yes, social media is important. As I referred to earlier, we have good engagement with some of the big social media companies to look at how they can provide advice as well.

Q148 **Chair:** If there were a quiz scam on one of the social media sites—Twitter or Facebook, for example—could you get the provider to close that down or find some way of dealing with that? Do you have both the technology and the powers to do that?

Ian Dyson: We can make requests, and we do have good arrangements with most of the providers. I talked earlier about phone lines and bank accounts. We have the same arrangements with Nominet, which is the .uk provider. Provided that we can give them the appropriate information and evidence that indicates that there is a fraud operating, they are very co-operative.

Q149 **Chair:** They are co-operative, but if someone posted a fake survey that meant they could get access to people's accounts, would that be easy to close down, technically? I just don't know. Is it something that the companies are on top of at the moment?

Ian Dyson: I don't think the technology is the issue; it is about us being able to—they obviously have an appropriate level. They do this across—

Q150 **Chair:** Do you have the legal powers you need? I know that they have thresholds now at which they close certain things down, like an abusive—these things with phone numbers and so on trigger something. Do you have the legal powers you need to ensure they act quickly on these sorts of scams?

Ian Dyson: I believe I do at the moment, yes. We have not seen an issue with that.

Q151 **Chair:** Okay. Presumably you can raise any concerns about legislation through the taskforce.

Ian Dyson: Absolutely.

Chair: While I am talking to you about some issues, we were talking earlier about the level of crime reporting, and you went through the figures in detail about the number of crimes and the number that get investigated at local level. There has been a lot of publicity recently about police stepping down investigations of crimes that affects non-vulnerable people. For instance, if there is a burglary of someone who is vulnerable, you might go round but, if they are not, you won't. Where does this fit into that stepping-down process? I can imagine that if you are a hard-pressed force dealing with a lot of physical crime on the spot, this might not be top of the list of priorities. Do you have any fears that it is being stepped down for that reason, or that it is being disproportionately stepped down compared with other crimes?

Ian Dyson: Policing has always prioritised case investigation and their service, inevitably. We do not investigate every absolutely every crime that is reported to us. Where I think this fits in is that we have invested a lot of time in focusing on the vulnerability of victims. So, with regard to the very point that people report to Action Fraud, we have trained all our call handlers to identify vulnerability—for example, if people are elderly, we establish whether they are on their own and so on. Then through things like Operation Signature, which you heard about in the Report—the Sussex-led initiative—additional victim care is provided. In London we have been piloting an economic crime victim care unit, which focuses on people who have an identified vulnerability but whose case is not going to lead to an investigation—if it leads to an investigation, they will get all the

victim care from that. That has been in contact with 6,000 victims since the pilot has been running and only one has been a repeat victim of fraud, which I think is very impressive. That is being rolled out across two other forces. As you know, the provision of victim services is a matter for local PCCs to commission, but we already have about eight or nine forces that are adopting Signature; they are slightly different models depending on local circumstances. Focusing on vulnerability across any crime type will benefit the work that we are trying to do, which is to say, "In this mass of volume, let's focus on the people who need the help most."

Q152 **Chair:** And the vulnerability will be judged on online vulnerability, because as we highlighted, some of the main victims of online fraud are not physically vulnerable, or those who have physical vulnerabilities, but they are young people, quite often.

Ian Dyson: That is absolutely right. That is why the economic crime victim care unit is focused on that issue—the vulnerability manifests itself in different ways from how it sometimes does with physical crime.

Q153 **Chair:** Let me pick up the issue of mule accounts, where young people are offered a sum of money to take over those accounts. Is that a big problem? What are you doing about it?

Ian Dyson: We have run campaigns to target the return to university and start of university term times. We sent out messaging and material to forces so that they can use that in their local university areas. We recognise that students are particularly vulnerable to running mule accounts. That is why we have focused on those.

Q154 **Chair:** Do you think the banks are doing enough on that?

Ian Dyson: The banks are providing a lot of information and there have been some very good TV campaigns by one of the banks on digital eagles and prevention. I think they are doing a lot to try and identify—

Q155 **Chair:** You talked earlier about the numbers you get from banks. Do you know if all banks are being targeted by this, or whether some are or are some are not? Is there a sliding scale of banks, with some doing better at tackling this than others? You said earlier that you did not have visibility of some of these numbers. Have you got any idea of whether it is being dealt with well in one bank and not in another?

Ian Dyson: Candidly, no, because if I was just to look at pure volumes, that would probably be as much a reflection of the number of branches and number of accounts that any particular bank operated rather than whether they are particularly more vulnerable.

Q156 **Chair:** Okay, that is interesting. I think there is a big issue about what information you have sight of. Talking of data and information, Mr Rutnam, how much are Government across the board providing data to banks or retailers or other organisations that do checks online, to try to prevent fraud? Are all Government agencies getting involved with that, as appropriate?

Philip Rutnam: What sort of data in particular?

Q157 **Chair:** I am thinking of, for example, immigration, where data checks take place; there are background data checks that can be shared. There can be a quick check to prove that someone has a valid British passport, that a passport is a validly issued one, that a biometric residence permit is valid, or that a driving licence is valid. Some of those can be automated checks. Is that co-operation happening fully across Government? Are all those agencies sharing data as they should be?

Philip Rutnam: So, I will say something and then ask Richard to say a bit more. I am aware of some information flows that are very important, such as the ability to check whether a passport or a biometric residence permit and so on are genuine. I do not know whether it is as comprehensive as it should be. I am aware that some areas—you mentioned immigration, for example—are seeking to automate and facilitate checks to make them much easier for banks to pursue.

Q158 **Chair:** Mr Riley, is it happening across the board? What about driving licences?

Richard Riley: I am not aware of a problem with driving licences.

Chair: It's just that Mr Rutnam mentioned them.

Richard Riley: I suspect, however, that it probably isn't as comprehensive as you might like. There might be some good reasons for that. There might be some legal—

Q159 **Chair:** I am interested in the fact that you don't know. The taskforce should surely be getting that bit right, as the Government are at the table.

Richard Riley: It has not been raised with me as chair of the management board that there is a problem with Government Departments applying data.

Q160 **Chair:** So if there were a problem you would expect it to be raised.

Richard Riley: Yes.

Q161 **Chair:** One thing we noticed in the hearing is that a lot of people were reluctant to give evidence. We had reports that some organisations were reluctant to give evidence that might not be complimentary about partners on the taskforce. Do you think that has any bearing on the truth?

Richard Riley: Not from my chairing of the recent meetings, no.

Q162 **Chair:** So people are being open and candid with you, at least in the meetings, even if they are not sharing the information with us and the public.

Richard Riley: Candid to a fault, Chair.

Q163 **Chair:** That is good news. What about globally, Mr Rutnam? Is there any experience of best practice in any other part of the world?

Philip Rutnam: Well, I am new to the role, but what I have gleaned—this may not entirely reassure you—is that we are very much leading the way globally. The existence of the Action Fraud reporting tool, the website, is pretty much unique internationally. Even the existence of reliable national statistics on the level of fraud and cybercrime is unique. The existence of the Joint Fraud Taskforce as a powerful public-private partnership is also unique.

Q164 **Chair:** So we are doing the best in the world.

Philip Rutnam: However, I don't believe that there are not things we cannot learn from others. Richard might have something to add.

Chair: Very diplomatic. I would hope there must be something we can learn. Mr Riley?

Richard Riley: Chair, we are certainly doing things differently. Whether we are the best or not is for others to judge. If you take America, for example, they are just introducing chip and PIN, so they are 10 years behind the UK. That might be for very good reasons, because the shape of the digital economy in the two countries may be different, but they are 10 years behind us.

Q165 **Chair:** Is anyone ahead of us?

Richard Riley: No.

Q166 **Chair:** Not even South Korea or somewhere? I say South Korea off the top of my head because they tend to be good at stuff.

Richard Riley: I don't know about the Korean peninsula. We don't think they are, but there is an onus on us to be the leader of the pack because of the size of the digital economy in this country. We have more people doing online shopping and online banking than other country, so I think there is a responsibility on the UK to lead. There are things we can learn from other countries in the wider financial sector, including money laundering. We are in lots of conversations with Australia and the US about their particular issues around the wider financial crime, but on fraud I think we are leading the pack.

Q167 **Chair:** Okay. We are leading the pack, but we know that lots of forces are doing it at very differing levels. You put a good face on it, Commissioner, about all the good work that you are doing, but it seems to be very slow rolling out. Is it mainly an issue of budget, resources or skills, or just a reluctance to put this crime high up the list because it is not so evident and visible to the public? Do you have any take on that? Do you have any suggestions about what we can do to try and push forces to take it further or about what the Home Office could do?

Ian Dyson: My thoughts are these. Every day I get press cuttings, and today I scribbled down four headlines that have appeared in different bits of the national media: "Hate crime at an all-time high"; "Police investigate 2,000 child abuse referrals in football"; "Knife crime up"; and "UK slavery more prevalent than was previously estimated."

Chair: Bit depressing, isn't it?

Ian Dyson: So, every force in the country is balancing what we have discussed this afternoon with those sorts of issues where there is real harm and real vulnerability. I think you are right about the hidden nature of online fraud, but the Joint Fraud Taskforce, however perfect or imperfect it may be, has raised the profile of this crime type, without a doubt in my view, across law enforcement, across businesses and across government. I welcome that, as somebody who has in the past sometimes struggled to get this on the agenda.

Q168 **Chair:** That is great. Because of resourcing, and all those other issues, is there more you think the banks and financial institutions, including the retailers, could be doing to try and stop this upstream? If you had a wish list now, what would you say they could be doing? What would you want to push them harder to do?

Ian Dyson: We touched on the issue of them reporting to us. I am cautious about saying eagerly that they should do so, because I am aware of the very real constraints about reporting under the current system, which, frankly, was set up to deal with the individual report. We have introduced a bulk tool, but it is still quite limited. But the new system we will bring in next year, or at the end of this year, will have the ability.

Q169 **Chair:** Would they need to report it to you if they gave you access to their information?

Ian Dyson: Sorry?

Chair: If you had access to what the banks know, they wouldn't need to report it in to a separate system, would they? Would you like that access?

Ian Dyson: We would prefer to have that single facility to receive all the reports, because it allows the system, rather than human analysis, to look at all the links and identifiers, because that one eBay fraud suddenly balloons into 3,500 victims, which is one case we've got. That would be success for me. What would success look like for law enforcement? First, greater consistency across law enforcement, which the work I've described to you, plus the HMIC inspection, will help us to move toward, despite all the competing demands. Secondly, being able to show that the crime survey for England and Wales is a good, independent assessment of a level of crime, and narrowing the gap between what is reported in that crime survey and what is recorded to police. Thirdly, focusing on the harm and having some assessment of it, to ask whether we are actually managing to reduce harm against the public. That would be a great thing for us to do, to have something like a national harm index.

Chair: It was interesting, going back to my brief time in the Home Office, that one of the targets was to reduce the perception of crime harm, which was a big challenge. I thank you very much for your time. The transcript will be up on the website in the next couple of days—uncorrected, as I said to the earlier panel—but you will also be sent one. Please do look through, in case there is anything factual that is misreported. We will be producing

our report—we hope—before Christmas, I can't give you an exact timescale. We will send you a copy of that just prior to its publication.