HOUSE OF COMMONS

Treasury Committee

Oral evidence: Economic Crime, HC 940

Wednesday 15 May 2019

Ordered by the House of Commons to be published on 15 May 2019.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Steve Baker; Colin Clark; Stewart Hosie; Catherine McKinnell.

Questions 837-915

Witnesses

I: Megan Butler, Executive Director, Investment, Wholesale and Specialists Division, Financial Conduct Authority, Chris Hemsley, Co-managing Director, Payment Systems Regulator, and Mark Steward, Executive Director, Enforcement and Market Oversight, FCA.

Written evidence from witnesses:

– Financial Conduct Authority, Payment Systems Regulator

Examination of witnesses

Witnesses: Megan Butler, Chris Hemsley and Mark Steward.

Q837 **Chair:** Good morning. I thank the panel very much for being here. I am going to ask you to introduce yourselves and say who you are representing. We are heading towards the end of our economic crime inquiry, on the retail side of things, and we are looking forward to hearing your evidence. Mr Hemsley, let's start with you.

Chris Hemsley: I am Chris Hemsley, the interim co-managing director of the Payment Systems Regulator. We are the independent regulator for the UK's payment systems, and in the context of this Committee's work, our focus has been particularly on the issue of authorised push payment fraud—a particularly unpleasant type of fraud that can have life-changing impacts on those who fall victim to it. Broadly speaking, what we have been doing is—*[Interruption.]* I'll stop there; that's fine.

Chair: Don't worry: you'll hear lots of questions asking you exactly that. Thank you for telling us who you are here on behalf of. Megan?

Megan Butler: I am Megan Butler. I'm the executive director of supervision at the Financial Conduct Authority, with particular responsibility for the wholesale market, retail investments, the life insurance market and some of our specialist supervision, including financial crime supervision.

Mark Steward: I am Mark Steward, the executive director of enforcement and market oversight at the FCA. Enforcement is what it says on the tin, I hope, and market oversight is our function of supervising primary and secondary market trading.

Q838 **Chair:** Thank you all very much for being here. Chris, you started to talk about APP fraud, which as you say has life-changing consequences for many of those caught up in it. Greater Manchester police recently said that scamming whereby money is fraudulently obtained is "the volume crime of the 21st century", snd obviously today we have had the figures from the Financial Ombudsman Service. Over 12,000 customer complaints about financial fraud were logged with the ombudsman in 2018-19. That was an increase of 40% on the previous year and more than double the volume received three years previously. Perhaps we'll start with the PSR. Is this a crisis?

Chris Hemsley: We recognise those figures. They are consistent with what we have seen, which is that there is a significant increase in this type of fraud. We took steps a few years ago to improve the collection of statistics and information about it, and this does paint a broad picture showing that there is an increase in this fraud, and it is quite a significant proportion of overall fraud. That is why we are taking steps in this area.

We see around 85,000 cases—that is from the latest figures available from UK Finance—so this is a significant problem, and one that we all need to play our part in addressing.

Q839 **Chair:** I will leave it up to you to decide, when I direct a question to the FCA, who is most appropriate to answer it, but where is this on the FCA's priority list? Does it consider this to be a crisis? Would the FCA agree with Greater Manchester police that this is "the volume crime of the 21st century"?

Megan Butler: It is certainly a very high priority for us. There are a lot of different statistics out there that try to size this problem in different ways, but the consistent message that comes through, although the numbers do not necessarily reconcile terribly well, is that this is a significant problem, and it is growing. That growth is often associated with the development of technology and the ability of some technology-enhanced scams/frauds to progress very quickly indeed with the use of technology. Yes, it's big; yes, it's growing; and it seems to be about developments in technology.

Q840 **Chair:** Does the PSR agree that the technology is causing these crimes to increase so much in volume?

Chris Hemsley: I think that is right. Those technological shifts deliver good things for consumers, but with them come new opportunities for fraudsters, so it is imperative that all of us work as hard as we can to keep up and close the loopholes. I agree with the general picture.

Q841 **Chair:** We will come on to look at preventive actions. In November last year, the FCA published an analysis of firms' data regarding financial crime. What were the key findings? Were there any surprises?

Megan Butler: I don't think there were any particular surprises. It was the first time we had gathered the data returned from 2,000 of the larger participants across the market, but spread across a range of different participants. The key message was consistent with what we have already heard this morning. There is a high level of concern around identity fraud, identity theft, phishing, mandate fraud and things of that sort that are coming through, so that was a big concern. Overwhelmingly the key area that firms are concerned with is cyber-related crime, which they would all say is existent and growing and a real problem.

There were various other pieces that we could learn from that around how the firms are responding to some of the challenges, because it also told us a little bit about how they make suspicious transaction reports. You can see a significant number being reported internally, but also onwards to the authorities, as well as how they are responding to individuals in terms of opening accounts, closing accounts and offering services, so we have much better sight of how the firms are responding to this challenge. It will get a lot more interesting as we are able to trend this data over time.

Q842 **Chair:** What about plans for future publication and how the FCA will track all this? We will come on to explore how you will work together and with many other authorities, including the police and law enforcement, but

what is the FCA's plan for, as you say, tracking this?

Megan Butler: That is exactly what we are going to do. This has given us a snapshot. The data we published last year was already based on 2017, so it does not give us a terribly clear view of how the firms feel now. That work is coming in now and we expect to publish that again towards the end of this year. As I said, that will give us a much better sense. One area that we are keen to push into is push payment fraud specifically. The categories we identified in the report that we asked firms to respond to was based on the Action Fraud bucket from a few years ago. It does not give us a very clear view of this particular fraud, which we are very keen to get a much greater sense of, so we think we might adjust the fields so that we get a greater sense of that for our next report. We are looking at that right now.

Q843 **Chair:** Perhaps the next question is for Mark. How will you hold firms to account? We will come on to explore the issues around gross negligence and some of the changes that are happening, but how does the FCA intend to raise the standards of what you expect firms to do to support customers?

Mark Steward: We require firms to have systems and controls in place, particularly around cyber-controls and internet usage. Megan knows exactly what we do in our supervision work to ensure firms are aware of that. We have had cases in enforcement where we have actually taken action against firms that have failed in this regard, and we have investigations. The one that we can talk about because it is finished was the Tesco Bank case. It failed to put in place the right protection in relation to a known scam that could make use of its technology to access customers' accounts, and we took action last year against Tesco Bank in relation to that. We imposed a fine that was calculated on the basis of the entire customer deposit base of the bank to send a message to the banking sector that they really have to get this right, because if they don't, potentially that deposit base is entirely at risk.

Q844 **Chair:** You obviously named Tesco there. I was going to ask you, without naming other banks—you're very welcome to name them if you like, but you might not want to—whether there any banks that are responding to the challenge particularly well. Are there any that are clearly outliers? Also, do you notice the difference between the different-sized banks? Are some of the smaller, challenger banks more nimble in dealing with this, or designing software answers, compared with some of our larger high street banks?

Mark Steward: Megan might have a comment on this as well. I don't think we see any significant differences between the traditional banks and the challenger banks. The entire sector is dealing with a need to step up and raise the game in relation to these sorts of protections. As you predicted, I am not going to name any names.

Q845 **Chair:** Of course. Looking at the regulatory and legislative landscape, are there any particular initiatives—regulations and legislative changes if there have been any; I'm not sure there necessarily have been—that

have particularly helped to tackle some of these issues?

Chris Hemsley: I can talk about some around the payment systems in general. We have been particularly focusing on the name checking change—confirmation of payee, in the jargon. This was originally identified as a change that would have a significant impact on a certain type of authorised push payment fraud, in which the individual thinks that they are paying a genuine party, but the payment is misdirected to someone else. That accounts for about two thirds of that type of fraud, on some of the figures that we have.

We recently issued a draft direction to put a regulatory backstop behind that to ensure that the six largest banking groups introduce that change in good time. Then, obviously, we will look for the rest of the sector to move as quickly as they can. That is quite a significant step. It clearly is not the whole part of it, which is why I briefly referenced the role that the code will also play, which I am sure we will come on to talk about.

Q846 **Chair:** Megan, has anything in terms of regulatory landscape or legal change really changed how these things are being addressed?

Megan Butler: One thing that I would call out, which connects to the publication that came out from the FOS this morning, was the extension of the FOS regime, and their remit to more clearly encompass the range of issues experienced by people who have suffered and been victims of push payment fraud. Those victims now have a greater capacity to go to the FOS to complain if their bank has not stepped up to the mark, or indeed if the payee bank has not stepped up to the standards that they are expected to meet. That might be one of the key reasons why we are seeing such a tick up in that number; we would have expected to see that, and I think it is coming through.

Q847 **Chair:** The payment accounts directive obviously sets out to ensure that all EU residents have access to a basic bank account. We heard evidence from UK Finance that it is quite difficult to refuse someone a basic bank account. Strict criteria have to be met for refusal. I do not know whether this a question for Chris or the FCA really. How difficult is it to refuse someone a bank account? I think some of the figures that the FCA published were the exact numbers of people refused bank accounts. I think we asked some of the banks when they gave us evidence about the numbers, which are clearly growing significantly, but are you getting feedback that it is still too difficult to say no to somebody when they ask for a bank account?

Megan Butler: I don't think it is difficult to say no in appropriate circumstances. I know the banks have a very particular view of this, but if they are properly considering their money laundering and other financial crime responsibilities, they can look at an individual, make proper decisions and say no in appropriate circumstances. I'm not sure that we are seeing it increasing particularly. One of the things in our financial crime survey was absolute raw numbers on how they are responding to this. The report said that a bit over 1 million customers had been refused access to financial services, and about 370,000 people have been off-

boarded. That feels like quite a lot, but it is a relatively small proportion of the overall number of customer transactions.

We will have a much greater sense of this issue as we see that number track over time. We quite regularly hear about individual cases of people who have lost access to bank accounts, sometimes in reasonably concerning circumstances, which we follow up with banks. I think they have every ability to make appropriate decisions around this, but they must not take decisions that are discriminatory, disproportionate or unreasonable.

Q848 **Chair:** We have heard evidence that it can be a bit burdensome to refuse. That is not a sentiment that the FCA would agree with.

Megan Butler: No, I don't think so.

Q849 **Chair:** Chris, any thoughts on the PSR?

Chris Hemsley: Our role particularly focuses on how the institutions then gain access to payment systems. There are broadly equivalent standards, so people have to act reasonably in taking those decisions, but it is a slightly different problem. That is definitely one for the FCA.

Q850 **Chair:** Do you see the number of people being refused access to payment systems? Do you track the numbers?

Chris Hemsley: Yes, we do. We have a particular role, which focuses on new institutions that are trying to get access to payment systems. There is the analogous issue of whether those institutions are meeting the appropriate standards. Yes, we receive individual complaints and summary statistics, and we obviously monitor that area. Again, I echo the general sentiment that people have to apply their compliance obligations. We don't see that that is a particular problem.

Q851 **Chair:** So where there is good reason, people are able to say no. Do you publish those numbers?

Chris Hemsley: Yes, we do. We are about a month away from publishing the latest set of statistics.

Q852 **Mr Baker:** Chris, you raised the issue of the impact of confirmation of payee. If I understood correctly, I think you were suggesting that two thirds of push payment fraud could be eliminated through confirmation of payee. Did I understand you correctly?

Chris Hemsley: I should probably be a bit more precise on that figure. The latest UK Finance figures are that there is about £350 million-worth of fraud under the authorised push payment fraud definition. About two thirds of that relates to this misdirection of payments. We think that confirmation of payee will make really good progress against that number. In the modelling and analysis that we have done, we have made the assumption that it could make progress on three quarters of that number. That would be reasonable progress. I don't think it will be the full answer, because fraudsters will adapt, and we always need to make progress and ask, "What's the next improvement that we need to make?". We expect it

will have a significant impact, but it won't stamp out this type of fraud, just by its nature.

Q853 **Mr Baker:** So you think, as an upper bound, it might eliminate three quarters of the two thirds of push payment fraud. Can you explain a bit more about how the modelling works, and why you drew the conclusion that it could have that benefit?

Chris Hemsley: In line with these sorts of decisions, we undertook an impact assessment and consulted on that. I don't want to be in the business of saying, "This is our forecast. This is what we definitely expect to happen." We tried to take some assumptions that we thought were reasonable and probably on the conservative side. We looked at the information available about misdirection fraud, and we then considered the scope of our direction and the possible impact it would have. There are some scenarios in there. On a conservative level, do we just increase the rate at which organisations comply, and will they eventually bring in these changes without our action, or will they act more slowly? That is the kind of scenario analysis that we did. That led to the benefits that we set out in our consultation.

Q854 **Mr Baker:** We probably agree that the victims are being psychologically manipulated in order to get them to send the payments. For the record, you are nodding. I'm grateful. Have you brought in psychologists to consider the extent to which confirmation of payee will interrupt that chain of manipulation from quite sophisticated fraudsters?

Chris Hemsley: The first thing to say is that I absolutely agree with you. When you start to read the case files and the information about these frauds, as I am sure you have, you see that they are incredibly sophisticated. We probably all know someone who has fallen victim to this type of fraud.

In direct answer to your question, I think that role is particularly one for the banks, when they think about the detailed implementation of this. We are setting out the outcome that we want to achieve. The nature of bank systems is that they are all a bit different; you have telephone banking and internet banking, and all the banks have slightly different systems. It really falls on them to ensure that the way that they comply and the precise design and information that they put forward in front of consumers actually works. We are going to have to stay on top of that because the techniques will adapt, so the types of warnings and process will have to adapt over time. That really is something for the banks to think about in implementation.

Q855 **Mr Baker:** What you have said is, of course, reasonable, but I am conscious that you said you had issued a direction to the six major banking groups that they are to implement confirmation of payee. I don't think you have closed the loop, and said the reason you are mandating it is because you have a high degree of certainty that it will be extremely effective, for good psychological reasons, in interrupting this manipulation. I am not sure you have said that.

Chris Hemsley: We do think this will have a significant impact. We are talking about the figures that I referred to before. It is probably worth saying a little about where this has come from. It has been thought about for a while. The payments strategy forum, towards the end of 2017, set out a broad design for confirmation of payee. That was the product of quite a lot of work, both from industry and consumer groups and others.

That engagement has continued. We think this is an important step. We have set out what needs to be done. There is support in our consultation actually. As part of our process, we consulted with all stakeholders and consumer groups offered their support. I think there is a broad sense that this a useful step.

Q856 **Mr Baker:** Would the FCA like to comment on the potential impact of confirmation of payee?

Megan Butler: We agree that it is an important part of the way that fraud can be disrupted and prevented. It is not going to be the only thing that will stop that. We need to recognise that there are other things that banks need to do, but this does play a significant part as an anti-fraud measure.

Mark Steward: There is one other preventative step that we have taken. It is mainly directed at more explicit scams and frauds, but it does cover the potential for online misdirection of payments. That is the information that we have put on our ScamSmart website and our ScamSmart campaign, which is designed to provide consumers with some readily digestible information on how to avoid being scammed. We continue to update that website with information, typologies and types of fraud that come to our attention, so that we can inform people of what sort of things to look out for.

Q857 **Mr Baker:** Picking up on what kind of things to look out for, I am conscious that sometimes fraudsters' phishing scams will use URLs in a web browser, which may be a couple of characters misspelled away from a legitimate domain name. You are all nodding because we all know that phenomenon.

What if the payee is just a misspelling, with one or two characters different? Would you think that confirmation of payee will have an adequate degree of checking to pick up that this is a small spelling mistake but a significant one? Can we expect that?

Chris Hemsley: Let me explain broadly how that will work, with the way that we expect it to work for internet banking transactions, as an example. If there is a perfect match between the account number and the name, you would expect the transaction to go through much as it does today, without any additional warnings or steps. If it is to an existing payee, you would again expect it to go through.

If you are setting up a new payee, that is when these checks particularly come in. With the name checking, ideally what we are looking for is, if there is a close enough match, so that it is Mr Smith rather than Dr Smith, for example, that there would be a warning. It would go back to the

customer and say, "Actually the name is this. Is this who you want to pay?"

If there is not a reasonable match at all and it is quite far away from it, you would expect the sort of warning that asks the customer to contact the payee again, to get the details right and restart or initiate that payment. There are those three things: trying not to slow down familiar, existing transactions, providing a proportionate warning when it is not quite right, and up the warnings when there is quite a bit of difference. The final thing I will say on this is that it is an area we need to keep under review. As the systems are put in place, people will learn from experience the sorts of matching that work. As you would expect, in the early days I think you will possibly see higher rejection rates than later on, as the system settles down. We also need to keep an eye on what fraudsters are doing, to ensure that the sensitivity of those warnings and the checking keep step with that. This is only the start of the process.

Q858 **Mr Baker:** To what extent have you thought through the dangers of false levels of comfort? The two examples I can think of are where the fraudster uses a payee name that is one or two characters out—as we discussed they might in a URL—or when perhaps a dyslexic person slightly mistypes and does not spot that they have. The latter is not such a problem, and a minor warning might be fine, but if the payee has used a typo to try to misdirect people, that might warrant quite a major warning. To what extent have you considered those phenomena, where people could get false comfort from a minor warning?

Chris Hemsley: You have set out a good range of the challenges there. The go live of confirmation of payee in version 1 is only the start. You have talked about someone who would be considered vulnerable under the provisions in the CRM code, so that is a good example of how, following the processes for someone who is vulnerable, they might not work effectively. Your other example was about the sophisticated nature of these fraudsters, who frankly convince people that the banks are trying to keep hold of their money. They will respond to the types of warnings and try to overcome that with their techniques and manipulation.

That is why it falls on all parties: there is the education piece, the bank's controls and the other checks and balances that we need to put in place to keep up with these fraudsters. It is not the end of the story; we need to keep working hard on this.

Q859 **Mr Baker:** I want to move on to what is going to happen when. You have published a couple of consultations. Can you just walk us through what you expected to be in place in April and July this year, and what you expect to be in place in December?

Chris Hemsley: In November, we set out a consultation on much of the detail of confirmation of payee. What we were doing in that consultation was checking two things: whether there was still a sufficient case for introducing the direction—we were proposing to introduce the direction, but we were consulting on that—and testing the dates that were originally

identified for confirmation of payee in that payments strategy forum in 2017.

During that consultation process, we used our powers to issue requests for further information from the banks, to understand more about their detailed plans for implementation. When we looked at those plans in detail and started to challenge them, it revealed that the banks were not ready to meet the dates originally identified by the forum. That was why we set the new dates in the consultation we issued in May with our draft direction.

In that process of consultation, we have now moved from a more general conversation about scope, coverage and direction to an actual legal text. We have now issued that as well. The consultation closes on, I think, 7 June, so we are quite close to that consultation's closing out and we will then be able to take our decision. If confirmed, that will mean that those six institutions and all the brands that fall under them will need to do two things.

First, they must be able to receive and respond to these requests: when you are putting in a transaction, the institution that you are putting that name and account number into needs to know where to go and have the information from the other bank to check whether the account name and number match. That is what will come into effect in December, and then March next year is the ultimate deadline for the other half—the requirement to actually make that check. Those are the two phases.

The first is quite an important step, because it then allows all other parties to move forward; there is only so much you can achieve by changing your IT, because you need the other parties to be able to respond. That is the December date. March next year is the date when we want those six banks to have definitely brought in the whole process. It goes without saying that we want other institutions to make progress on this, and that is obviously the next focus of our activity.

Q860 **Mr Baker:** As a software engineer, I look at it and think you give a unique number—all right, it is a two-part unique number—and look up a name. It is really trivial, conceptually. Could you give us an idea, in layman's terms, why it is complex for the banks to deliver what is conceptually a trivial look-up?

Chris Hemsley: One of the challenges is to ensure that there is a co-ordinated approach to those data standards. If you have two parties it is relatively easy to get them together and understand how to interface between those two systems. It is much more challenging when you are considering setting a standard that needs to work for in excess of 100 payment providers. That is at the core of some of these challenges on standards. Ultimately, the individual IT systems all then need to be updated. That in itself, because of the legacy systems and the range of different systems that exist, is much more complicated.

Q861 **Mr Baker:** That is what I was driving at. Is it the case that the banks

have legacy systems that do batch processing on mainframes from perhaps decades ago, and you are now asking them to deliver something that works in real time?

Chris Hemsley: Those are some of the challenges. Some of the banks are in a better place because of the way they have chosen to update their systems, which is why we had to take the time to scrutinise those plans in detail. It is very institution-specific.

Chair: That is very helpful. I think we will return to that. We are doing a separate inquiry on the IT resilience of banks, and no doubt all those different systems laid on top of each other is very much part of that.

Q862 **Colin Clark:** What are the banks currently doing to combat money mules, and what more do you think banks should do?

Megan Butler: Money mules are an area of supervisory focus for us at the moment with the major banks. That started earlier this year and we expect to do more around that. Money mules are a function of two things. First, banks are around client account opening, so we expect them to have proper "know your customer" arrangements, which stop a certain number of mule accounts opening in the first place if done in an effective way.

However, we quite often see mule accounts that open ostensibly perfectly legitimately and then change over time to become what we would call a mule account, which is why it is so important that banks have effective transaction monitoring arrangements around what actually happens in accounts. "Know your customer" tends to be associated with current account openings, but its transaction monitoring is also important for knowing what customers are doing. That is what we expect of them, and it is what we expect should prevent the proliferation of mule accounts. It is a major issue for us and, indeed, for banks at the moment.

Q863 **Colin Clark:** We have read evidence that students are sometimes conned into being money mules. Surely the banks can spot that a movement of cash is very unusual? What is a typical example? Why is the banking system not picking up on it faster?

Megan Butler: They do pick up on a certain amount of these, but this is one of those areas where technology is likely to be particularly helpful, in terms of transaction analytics. Interestingly, we are seeing some examples of that coming through the FCA sandbox as banks explore how to develop transaction analytics that can be applied to this type of thing. An awful lot of what we observe on transaction monitoring is still manual. They have a much smaller chance of finding this type of activity if it is a manual process, so we need a much greater emphasis on technology solutions for some of these things.

Chris Hemsley: I would just quickly add that that is on the firm-specific side. The payment systems themselves can play an important role. Last year, new systems were rolled out so that the payment systems more generally are able to track money as it moves between different accounts. Obviously, that helps the fight against mule accounts.

Q864 **Colin Clark:** Following on from that, how soon after an account is identified as receiving stolen funds do you expect the bank to prevent future payment from being received? How quickly should banks recognise it and close the account down? This is moving on from money mules and cons that are going on. What expectation would you have?

Chris Hemsley: We want all institutions to play their part, so everyone needs to act as quickly as possible. One quite encouraging change that happened last year were the changes that were put in place to improve the way that banks talk to one another. They agreed standard ways of passing information to one another, which facilitated the receiving bank acting more quickly on these types of frauds.

The other thing that is important in this area is that as we move towards improvements in how banks reimburse victims who have done nothing wrong, that sharpens up the incentive. You have that information that allows them to act and then that firm financial incentive.

Q865 **Colin Clark:** But that is only in the case of banks compensating. Banks don't always compensate on authorised push payment.

Chris Hemsley: As we are making this journey to a better approach that protects people more appropriately, encouraging people to act much more quickly will be part of the picture going forward.

Q866 **Colin Clark:** The reason I ask is, and you will be well aware of this, that the *Daily Mail* recently exposed an overseas gang who were impersonating HMRC and threatening victims with immediate arrest if they didn't make payments. The *Daily Mail* journalist then paid money into the accounts eight weeks after customers had warned that those accounts were fraudulent. Some of the money was blocked, but why are some banks acting faster than others? I was listening to what you were saying to my colleague. Is there some sort of historical reason? Are the systems so chronically out of date that there is this inconsistency? Surely it is the same questions that each of the banks are asking.

Megan Butler: It is the same question, but their systems are very different and their ability to spot it is very different at the moment. Their response frameworks are different. That is why the code has the capacity to achieve a step change in the way they think about this within their banks—I know we are going to get on to the code in a moment.

In terms of setting particular standards, such as you have to respond within x days or x hours, generally we want banks to exercise judgment and to be capable of responding properly. The difficulty with setting hard and fast rules around this is that they then work to the hard and fast rule and not necessarily as quickly as they should in some particular circumstances.

Q867 **Colin Clark:** But the *Daily Mail* exposed that this was eight weeks later. Consumers contacted the newspaper, the journalist had time to put through a payment, and eight weeks later somebody else could be conned to the same extent. I can't grasp how it takes eight weeks—

actually, I can't grasp how it would take one week.

Megan Butler: Without commenting on that particular case, we would expect firms to have systems and controls that would respond to a heads-up that they have a fraud.

Chris Hemsley: I guess there is also the change that Megan talked about earlier, about the receiving banks now being within the scope of the financial ombudsman. This is a really good example of that. It allows the financial ombudsman to consider whether the receiving bank acted reasonably. I am not going to comment on that individual case, but you would obviously expect the Financial Ombudsman Service to ask some fairly serious questions, if that case was referred to it.

Mark Steward: Can I round out the picture? A lot of that is to do with prevention and remediation. There is also a very strong aggressive pursuit strategy to do with money mules. That piece of work has been taken up by the National Economic Crime Centre and co-ordinated between us, the NCA, HMRC, the SFO, City of London Police and the Crown Prosecution Service. A lot of work is being done to deal with not only the prevention side, but the pursuit of what lies behind the money mules.

There is information on the ScamSmart website to help people identify when money mules might be used. In some awful scams the fraudster has conned someone. Then, in order for the victim to get their money back, the price they have to pay is to allow their bank account to be used for another fraud against someone else. There are some terrible stories, and publicising such stories and making them more apparent on websites such as ScamSmart helps people avoid them in future.

Q868 **Colin Clark:** I think the problem is that our constituents and consumers would expect this Committee and this Parliament to protect them in the first place. Having spent a lifetime in business, I find it incredible. I would not have been able to hang on to any customers if I had let them down to this extent. Gareth Shaw from *Which?* magazine said that the "banks are neglecting to do even the bare minimum". Consumers must be flabbergasted after all these years. These look like relatively unsophisticated frauds: somebody phoning or contacting people with a very clever script and convincing them to pay money across. In this day and age, with the sophistication of iPhones and internet banking, it is a pretty basic con—this must date back to the Victorian period. I am absolutely shocked that we, as representatives of constituents, are still failing to protect them. We keep speaking about doing something after, but by that time somebody's life is completely ruined.

Chris Hemsley: This is why we have been taking this incredibly seriously. I keep talking about it, but the code brings in additional protections in this respect. As long as the customer has acted reasonably in those sorts of cases, there is a time limit of 15 working days on refunding the money, and the banks then have to decide who effectively is to blame and sort that out. It should make a real difference to the timelines and the general level of protection afforded to consumers. That is why I take this

opportunity to welcome the fact that seven banks have already committed to signing up to that code. It is a really important step forward for us all.

Q869 **Colin Clark:** Is there an imbalance between convenience, technology and security? In offering consumers convenience, speed and timeliness, are we actually exposing them to a massive security risk? Have we actually left the safe open and handed the keys over to a third party? Therefore, should we not be rolling back and saying, "You can't do this unless you can guarantee security"? We have possibly already gone too far. Consumers have asked for this convenience, but did they realise what the exposure was? Did they realise the risk to their security?

Chris Hemsley: I think this is a really good debate to be having. What we have seen is the modernisation of our payment systems, and with that has come greater speed. For a range of day-to-day transactions that are lower risk, you want to maintain that speed. It is in the business's interest and the consumer's interest—the convenience of tap-and-pay, for example. When you look at larger scale transactions to new payees who are overseas, you start to get these flags. Surely there must be a way to take a different approach between those two. There are circumstances in which consumers want larger payments to be absolutely instantaneous—when you are buying a house and things like that—but by and large, a lot of consumers would welcome a bit more friction in the system for those high-risk payments.

Q870 **Chair:** Colin mentioned the *Daily Mail* investigation, and the article specifically mentions the four banks. It says that "payments from Lloyds and Santander accounts did not go through", but NatWest and HSBC did allow attempts to move cash. When you see an article like this and people are named, does the PSR call them? Does the FCA call them and say, "What's going on?"

Megan Butler: I am not sure whether Chris's team would call them, but we definitely would.

Q871 **Chair:** Did you in this case?

Megan Butler: I am not going to comment on a particular case, but when things are brought to our attention—be it in a newspaper or otherwise—we will follow up and understand what has caused it. If there is a problem, we will make sure it gets fixed. It is really important—just coming back to the earlier conversation—that we have a strong focus on prevention, and not merely on reimbursement. There is an awful lot of evidence that shows that even if you get your money back, you are so inherently damaged through the process that it absolutely undermines your confidence, so we can't just have a reimbursement strategy; we have to have a prevention strategy.

Q872 **Rushanara Ali:** Good morning. The FCA and PSR were observers on the contingent reimbursement model steering board, and the CRM has set out the circumstances in which the victims of APP scams—sorry about all the acronyms—would get their money back and from whom, with a practitioner guide to follow. What do you believe the CRM will mean for

victims of APP fraud? Perhaps you can start, Chris.

Chris Hemsley: Well, first I will apologise, because we probably created many of those acronyms in the first place.

At the simplest level, this really is a step change in the protection available for consumers in respect of that authorised fraud. There have been existing processes and rights for unauthorised payment fraud; it is the authorised bit that has changed. Again, from a consumer's perspective, what they will see under the code is that they can contact their bank, as they do now; there is a deadline as to when the case needs to be considered; and if they have acted reasonably, they will get their money back. On one level, it is that simple. And then the banks need to—

Q873 **Rushanara Ali:** But it is voluntary. What are your views on the fact that it is voluntary? Some hold the view that that will reduce its impact. How many banks are involved? Do you have a list of banks that have not joined but are likely to? What are you doing in the current situation, given that it is voluntary, to try to encourage them, shall we say?

Chris Hemsley: In terms of the voluntary nature, the group started their work in April and delivered in February a code, which is now being implemented, so I think that voluntary approach has actually meant that this issue has been taken forward at a reasonable speed. I put on the record my thanks to all those who have been involved in that—the consumer groups and the banks that have participated. So I think there has been speed. The other aspect of your question is: what next? We have had the commitment from seven that they will sign up from day one. I do hope there will be more.

Q874 **Rushanara Ali:** Do you have an idea of others that are in the pipeline and planning to join, and what are you going to do to encourage them to do so? We are going to come on to regulation, but at this stage what are you saying to them? Are you saying, "Join, or regulation might follow"? I guess I am talking about the carrot, because at the moment it is just about carrots. Is there a stick behind this to try to encourage them to join?

Chris Hemsley: We absolutely want other institutions to join, so we are encouraging them to do that. In carrot mode, we think these are important protections. I think it is also—

Q875 **Rushanara Ali:** How long are you in carrot mode? I don't actually like carrots, but anyway. What is the timeframe for where you would like to get to? Obviously, if it can be done in this way, fine, but there are some issues with the effectiveness of a voluntary code.

Chris Hemsley: Of course. On 28 May the code will go live, and we hope that more will choose to sign up. It is also worth saying that the code is very explicit that it does not stop anyone going further. We have also seen other institutions that have taken steps to protect their customers. TSB, for example, under its fraud guarantee, has chosen to take action.

I think that is quite a lot of progress, but more is needed. I think part of this is about being clear about the protections that are available for consumers and the fact that the institutions that have chosen to sign up to the code, or that have provided other forms of guarantee, have a different proposition for their customers; they are offering greater levels of protection.

Q876 **Rushanara Ali:** Yes, but we are very concerned about the ones that are not part of this code, so what we are doing about them? There is the point about negligence, for instance. Some banks are reported basically to have accused their customers, in these situations, of negligence. If they are marking their own homework, how can you be confident that our constituents are being protected in those situations? This is the frustration with the FCA not actually using the stick, perhaps. How long do we have to wait before more banks join in? Colin made a point about the tension in regard to the technology. The advances in technology are useful, but the risk management doesn't seem to happen fast enough, as far as our constituents are concerned. Perhaps others can come in on that.

Mark Steward: On the stick, we can't force banks to join up to the code, because it is voluntary.

Q877 **Rushanara Ali:** But you are the regulator.

Mark Steward: We can't; we don't have that power.

Q878 **Rushanara Ali:** I am asking whether it should be—

Mark Steward: That would require legislation.

Q879 **Rushanara Ali:** That is fine; we are parliamentarians. We would like to know what the steer to us is. What is the timeframe by which we should be looking to push for legislation? What is your view on that? We have gone around in circles in some of these debates. This is an opportunity for you to tell us. Otherwise, what happens is that we spend quite a lot of time on this. It is great that banks have joined, but gratitude to banks that have failed to protect our customers is not really enough. What is the answer?

Chris Hemsley: TSB is taking steps, and the code is being implemented in two weeks' time. That is a good, timely response. If we don't see further progress on mitigating fraud and, over time, more people signing up to these standards so that they become established as industry best practice, we hope that the financial ombudsman will increasingly see them as the standards that will need to be applied in any event. We will be monitoring how the code works, the impact it is having and the number of parties that sign up. Of course, we will continue to work with the Government. If legislation is the only way to plug the gap, we will of course talk to the Government about how to take that forward.

Q880 **Rushanara Ali:** Thank you. In terms of the timeframe, do you see it being a year or two, during which you will stick to the voluntary code and see how it progresses? Is it one year or two years? At what stage do you

start saying to the Government, "We have taken this as far as we can with the voluntary nature of it, and now these things need to happen"? Is it in a year's time or in two years?

Chris Hemsley: The first thing to say is that the Lending Standards Board has a role in monitoring the code implementation. We will be monitoring how it goes. If we don't see progress being made on these frauds, we will act quicker. We are not going away and coming back in a year to check; we are keeping a very close eye on this.

Q881 **Rushanara Ali:** But you will have a review in a year's time to look at how progress is being made so that you can draw some conclusions and we can benefit from that.

Chris Hemsley: Yes. We report annually anyway. I guess what I am saying is that we will be keeping it under review much more closely.

Q882 **Rushanara Ali:** That is brilliant. I just have a couple of questions on de-risking. You are all familiar with some of these issues. I was involved in a campaign with charities and money transfer businesses a few years ago, and I am grateful to the FCA and others for some of the guidance that was issued to try to help businesses that sometimes unwittingly find themselves in that situation. In cases where a bank decides that it has to do an investigation, because of the legislation, its ability to prove itself and know what is going on is quite limited. I understand the legal ramifications of that, but if you are a charity or an affected individual, you could just get a letter saying, "Your bank account is now going to close." There is obviously tension in targeting and getting those who are breaking the law, versus those who are innocent. Is there sufficient protection, so people are able to prove themselves otherwise, given the lack of information that they are going to be party to?

Megan Butler: From our perspective, we need banks and other financial institutions to tackle money laundering and financial crime. That does lead to individuals being debanked or having transactions refused. We are aware of that. I have to say that we don't see these two things as inconsistent; these two regimes do not operate in tension. If banks are looking at this properly—that is, taking individual decisions around an individual, rather than bulk decision making—they should be able to take appropriate decisions.

Q883 **Rushanara Ali:** So they are not doing that anymore? They are dealing with it on a case-by-case basis?

Megan Butler: We would expect them to.

Rushanara Ali: Are they, though? Do you know whether they are?

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

Q884 **Chair:** There are whole sectors that are being debanked or derisked.

Obviously, some are vulnerable sectors; Rushanara has mentioned money transfer businesses, but pawnbroking is another one.

Megan Butler: Yes, and if banks are purporting to derisk entire sectors for financial crime reasons, we would say they are not doing proper "know your customer" arrangements, because those are all about knowing the individual and making an individual judgment. This should never be a bulk process, and that speaks to the point we made earlier that it should be non-discriminatory, proportionate and reasonable.

However, there is always the tension, which you have called out: the ability to give reasons to people. While we do come across cases where we cannot understand on any reasonable, proportionate basis why an individual lost their access to whatever financial services they were looking for, in other cases we come across we understand entirely why that happened, but equally we understand why that reason cannot be offered to the participant, for all sorts of tipping-off type reasons. I recognise that there is a tension in there.

Q885 **Rushanara Ali:** Yes. Obviously, I have followed this very closely and fully understand the tensions. The question really is, what do we do about it? It is not fair to those who are innocent and are caught up in this blanket response, and you cannot give us a guarantee that the FCA is doing enough, first, to tackle the blanket-response practice of some banks, despite all the work that has been done over the years. We need to understand what further you can do to address. Secondly, on monitoring, you have 1.1 million prospective customers for financial crime-related reasons. That is interesting. Then there are 375,000 existing customers who are turned away because of those concerns. Who is doing the monitoring to understand the profile of those people by nationality, by ethnicity, by social class or by vulnerability? That links to the money mules point. How do you get to understand where there is discrimination going on, in terms of both types of business and characteristics? Is the Equality and Human Rights Commission engaged with you in working that stuff out?

Q886 **Chair:** A brief answer please, as we need to move on.

Megan Butler: A brief answer is that the key to this, for us, is better data so that we can see this. You have seen the statistics that you have drawn from our "Financial Crime Report". That was our first cut through that the banks are giving us. We will get a great deal more information coming through following the Payment Account Regulations coming into force on what the banks themselves are doing about refusal of bank accounts. When we have that, not only will it give us a sector-wide view of trends, which is interesting, but it will give us firm-specific views on whether there are characteristics across that that would cause us concern, and all those features that you have articulated will give us very great concern if we see that operating.

We will have better data and we will be able to respond on a less case-by-case, which we feel by its nature does not get to everybody quickly enough. We will get much better data, which will allow us to tackle some

of those broader societal issues in the right way and, importantly, get the banks to tackle them in the right way too.

Q887 **Stewart Hosie:** Chris, we have seen evidence that some economic crime is committed when there is a third-party data breach—BA, Ticketmaster—or in circumstances completely out of a bank's control, such as a fraudster using number spoofing. What discussions have you had, or what discussions have been had between the regulators to address those issues?

Chris Hemsley: I will make a start—I know the FCA is busy in this area as well. In particular, there is the development of this code, which is both from the reimbursement perspective, which we have been emphasising, and to mitigate and reduce these frauds in the first place. That involved a number of different regulators, Government Departments and law enforcement, as well as consumer groups and others. That was one way of engaging to get an appropriate understanding of some of the challenges.

This is certainly an area where there is always more to be done, and an area where, as part of the work plan that we are undertaking now, we have been engaging with our fellow sectoral regulators—energy, water and so on—to carry on the conversation to identify what more could be done.

Megan Butler: That is exactly the right issue, around how regulators can work together here. We can get our hands around the regulated financial services community, but everybody needs to play their part in this piece, which is why we work very closely with, in particular, the Information Commissioner's Office around aspects of this. An awful lot of those parties will be subject to those regulations, as opposed to ours.

Q888 **Stewart Hosie:** On that point, what information can currently be shared between the regulators when you find out about a data breach like that? What can be shared between you and between others at the moment?

Mark Steward: We have an MOU with the ICO in particular that covers gateways around information sharing both ways, so that we can be in regular dialogue with one another, and we can work together as well, because there is often going to be an issue in our sector when there is an issue in their sector, or vice versa. There is co-ordination. There is a mechanism and a protocol for that to occur, and we are doing it.

Q889 **Stewart Hosie:** Does that data sharing within that protocol also include private businesses if they have been the subject of the data breach?

Mark Steward: I think it would include information where, for example, the ICO might be aware of a data breach in a private firm through its work that may have an impact on our work. There would be provision for that to be shared with us.

Q890 **Stewart Hosie:** In the case of both the FCA and the PSR, when one of these large third-party data breaches happens, which may then lead to a fraud taking place within the banking sector, are your organisations advised early that it has occurred, or do you find out only once it hits the newspapers?

Megan Butler: There is a very high level of information sharing in the context of cyber-breaches between authorities and from security services and other forces around how that might connect, because all these things at the end of the day usually manifest as harm in the banking system, because they result in money flows. For all that information, there are structures and a high level of information sharing well before they hit the press.

Q891 **Stewart Hosie:** When you were talking earlier, in response to other questions, about requiring data to do analysis you seemed to indicate that there isn't a shortage of data or shared data when it comes to these third-party data breaches. Is that correct?

Megan Butler: There will be circumstances in which it is visible to others that there has been a third-party breach. There is always the challenge of a third party having had a breach and not talking about it, which is a challenge—or not knowing, which is equally challenging. Those are endless challenges, particularly if they are not within the UK. Increasingly, in this global world, some of the key data breaches happen offshore, at which point the ICO's powers, rules and oversight will not bite. We have challenges there, but if they are within the jurisdiction and within that remit, and they come to attention, there is a strong and established mechanism for information sharing.

Q892 **Stewart Hosie:** There is a longer discussion to be had—not today—about where data servers are housed, physically and in jurisdiction terms. We may come back to that or, if you have some real concerns or issues about that, could you write to the Committee? It would be helpful to see whether there is anything there that we need to pick up on.

In terms of these third-party data breaches and the economic crime that follows from them, do you believe that other, non-financial, sectors, such as technology companies, should shoulder some of the financial burden where data breaches have occurred? Do you think that third-party or non-financial sector businesses should be sharing some of the burden on this?

Mark Steward: It's quite a complicated question. We are aware that many of the scams and frauds that we detect or get reported to us occur online, so they are marketed through online platforms, such as Google. We can put information on our ScamSmart website about what the scam or fraud is. We can put the name of the firm on our warning list, so that people can be aware to watch out. What we can't do is stop that website from remaining visible and accessible to the public.

Q893 **Stewart Hosie:** Why not? A fraud has been committed. Why can't you tell the police and have them shut it down? They would be quick enough to stop someone advertising the same scam in the back pages of a newspaper, would they not? Or would they be allowed to do that?

Mark Steward: It's up to the publisher or owner of the site to decide whether to allow an ad or a piece of marketing to occur on their platform. We don't have the power.

Q894 **Stewart Hosie:** Does Google's advertising sales team have the necessary expertise to say, "No, sir, we are not going to take your fraud advert"?

Mark Steward: They are probably not in the business of detecting fraud, if that is what you mean. I think that is probably right.

Q895 **Chair:** They're not going to say no, are they?

Mark Steward: We certainly have conversations with Google, where we see things that really need to be taken down. Sometimes we get the right answer and sometimes we don't.

Q896 **Stewart Hosie:** There is clearly a piece of work to be done there, as well. On the number spoofing issue, I understand it is remarkably straightforward, which is quite scary. Presumably you are discussing it with all the mobile telephone companies so that people can't spoof a number. Are you?

Mark Steward: Yes, I guess that's right.

Q897 **Stewart Hosie:** What have they said? Why is this still possible technologically?

Mark Steward: It's a complicated question because it involves—

Q898 **Stewart Hosie:** It isn't complicated. If I'm a fraudster and the telephone number that comes up on your phone when I call you is the main office number for a big bank, it is not a complicated question at all; it is a crime. Why is that still being allowed to happen? Philosophically and practically, technically, why has that not been stopped?

Mark Steward: I am not sure we are the right organisation to answer that question directly, because it involves a lot of other agencies.

Q899 **Stewart Hosie:** That was the starting point: the interrelationship between the regulators. Is somebody speaking to Ofcom?

Chris Hemsley: As part of that process of working with our fellow regulators, we have started talking to them. I don't want to mislead the Committee on whether we have spoken to Ofcom or not.

There is another part of this; there is a bit of a journey here, a process. The first thing is that under the code, where the individuals act entirely reasonably, they are not liable. The liability then moves on to the banks. One of the effects that will have over time is to sharpen that incentive to take action.

The immediate action may not be for the banks. They may need to work with other sectors. I think it falls on all of us regulators—the PSR and others—to follow that and take action. There is stuff to be done, but it is a really good example of where we can't stop.

Q900 **Stewart Hosie:** A final question. Do you think this Committee should be doing some more work in that area with the non-financial regulators?

Chris Hemsley: I think there is more work we can do. I think there is more work to be done, and that cross-sectoral issue is one that you should consider. We are obviously focusing on making sure that the changes that we have in place, and that are coming in, work effectively. Looking at the other root causes of fraud is obviously where we all need to keep co-operating.

Megan Butler: I agree with that.

Q901 **Chair:** Before I bring in Catherine, on Stewart's question, in the same way that I asked you about the banks named in the *Daily Mail* article, when we took evidence on TSB last year in relation to mobile phones and the way that people have access to accounts, EE was one of the companies through which people had been able to obtain SIM cards and take over people's phones and everything else. Do you phone up EE—or, without going into specifics, phone companies—and say, "Hang on a second; we have a really serious financial fraud issue going on here," or is that something that you would hand over to another regulator? I guess the question is whether we need to get the other regulator in and ask them some questions.

Megan Butler: The short answer is that if there is another regulator, we would probably hand it over to the other regulator. In the context of EE, we would probably hand it over to Ofcom or somebody. If you are talking about a Google or a Facebook, we would probably call them directly, because there is nobody obvious we could otherwise talk to who would have greater grip than we might.

Chris Hemsley: There is also the joint fraud taskforce, which has that broader membership. It is worth remembering that they are in this space as well.

Chair: That's very helpful.

Q902 **Catherine McKinnell:** I guess the other side to this is the customers. On the balance of customers being held responsible for the actions that they take in response to what are clearly very sophisticated frauds, I think it is right that much of that falls back on to the bank, and the code is increasingly providing for that. However, an element of education is also required. Banks will be interested in their customers becoming better educated about even sophisticated frauds, so that they can be avoided. Where do you think we are, in terms of responsibility for, and the success of, customers being educated about fraud?

Mark Steward: That speaks to the ScamSmart agenda. The FCA does not have a general consumer education remit, but I think we have an obligation to help consumers avoid becoming victims of frauds and scams, which is what the ScamSmart campaign website is all about. It started about three years ago, and we have conducted a number of campaigns to promote ScamSmart through television, radio and newspaper advertisements, designed specifically to address the issue that you raised: how can people better protect themselves, and what sort of information do they need to know about how scams and frauds operate? It sounds like

basic information, but it is basic information that people often forget about when they are being induced to make an investment by someone who turns out to be a fraudster or a scamster. It is information like: beware of the glossy brochure, and beware of the investment where you cannot kick the tires to make sure that it is really true and is really there. It is information about pressure selling tactics—being forced to make decisions really quickly—being given guarantees, or being offered very high returns that look too good to be true.

That kind of information needs to be repeated over and over again to really get it through to people, so that they understand that they are at risk of being scammed. We know that, and there are things that people can do to avoid it and prevent it.

The other aspect of ScamSmart that is under-recognised is what it is doing to humanise the victimhood that people who are subject to scams feel. People who have been deceived, scammed or defrauded often do not like to talk about it. They don't like to report it or come forward. They feel embarrassed, silly and stupid. That shame is part of the experience. ScamSmart is also trying to make it clear that this could happen to anyone. It doesn't just happen to people who are incompetent or gullible; it happens to very sophisticated people, too. You only have to look at what happened with Bernie Madoff to know that that is exactly true—it can happen to anyone. The more information we can collect about what is actually happening in our society and what scammers are really doing, the better we are able to protect ourselves.

ScamSmart has been enormously successful. It has generated a lot of information for us, as well as a lot of attention, in terms of people clicking on the website and getting help. They can get further help from the website, including from our contact centre.

Q903 **Catherine McKinnell:** ScamSmart is focused on investment fraud, rather than wider economic and banking fraud.

Mark Steward: Yes. It will include app fraud, but it won't include the man who knocks on the door and wants to install new windows.

Q904 **Catherine McKinnell:** Or makes phone calls.

Mark Steward: It includes phone calls.

Chris Hemsley: There are other initiatives as well. UK Finance has been promoting the "Take Five" campaign, which also helps charities and other local authorities to take part by providing them with materials.

Q905 **Catherine McKinnell:** I guess the question really is, are we getting the balance right between the responsibility that consumers have to take for their own actions and where the banks currently are? We have heard about so many people who have been victims of this fraud. As you say, some people have been left in dire circumstances, and they don't particularly want to talk about it. The people who have come forward have done so because their experience has been so traumatic for them.

Do we have the balance right between the responsibility that the banks are currently taking for these frauds and the consumers who have been left to bear the consequences of sophisticated fraud?

Chris Hemsley: On the authorised push payment fraud, we were concerned about that balance. That is fundamentally what the problem was, and is today. If the banks had technically carried out the instructions correctly, that was the end of their liability in this area, which was the minimum standard of the law—not that that is what banks were doing, but that is what the legislation provided. That is why the code is a significant shift.

It is always difficult to describe the balance. It is fair to say that expectations on banks as sophisticated organisations are much higher than those on consumers, but both parties need to play their part. That is why it was really helpful that we had three or four consumer organisations—Age UK, Toynbee Hall and others—involved in the development of the code to try to strike the right balance. It is a difficult one to address. We expect to keep it under review. Let's see what is happening in practice to judge whether we have the balance right. The main thing, which is really good news from my perspective, is the significant shift in the protections available on authorised push payment fraud.

Q906 **Catherine McKinnell:** It's just frustrating, because it's a bit intangible at the moment. Obviously, we have seen the new code, but it would be good to understand the timeframe in which you will be looking at this to see whether the steps taken have carried us far enough in the right direction. There is another aspect, which is that younger people—students who are vulnerable and have just moved away from home with a new bank account—are being targeted, not just for fraud, but to participate in fraud. Is enough being done to educate people in schools before they leave home and become a student? Are we doing enough? Is there more that could be done within the education system? Is there more that the Government could do to support a collaborative effort to make sure all young people are educated about financial crime and fraud?

Megan Butler: From our perspective, what is clear in all the work we do around consumer education is that you can't do it just once and target it at a group. You have to do it continually and for everybody. You have to have it in messages that each person or group can understand and relate to. That would indicate that there is a broader need to keep communicating about that and upskilling people about their decision making. That is for all portions of our society; it is not just about talking to a 16-year-old or someone at 55 who is making pension decisions. We have to keep finding mechanisms all the way through people's lives.

Q907 **Catherine McKinnell:** But there is simply nothing happening for young people in schools and in the education system.

Mark Steward: Not from our perspective at the FCA, but the National Economic Crime Centre, which has really only just started, is pursuing a multilateral strategy to attack economic crime in its broadest sense. That

will include a prevention strategy, which is probably where, from a whole-of-Government, whole-of-UK perspective, that debate around what can be done to educate really needs to happen. It is something that we will be talking to the NEC about.

Q908 **Chair:** I mentioned earlier that the Greater Manchester police talked about economic crime being the volume crime of the 21st century. I thought it was very interesting; they also used another phrase. They were looking at a lady who they said had been groomed and exploited relentlessly. It was not just a one-off email that, if you'd thought about it, you'd have thought didn't look quite right. It was systematic grooming of this particular person before they transferred hundreds of thousands of pounds. Is that a trend that you are seeing?

Going back to working with other regulators and the grooming we have seen in other crimes, such as encouraging people to go abroad and join ISIS, do you think there is some learning that could be taken from how police and others have dealt with grooming that could be useful for tackling economic crime?

Megan Butler: That's a very interesting thought. Coming back to the UK Finance statistics they published, they were seeing in the breakdown those romance crimes, and things of that sort. It clearly is a growing area of crime.

It comes back to an earlier comment: some of these things have been around an awfully long time. They have a technological overlay now, but they are dealing with the same levels, the same human vulnerabilities that have been exploited for ever. Some aspects of that are things that law enforcers, regulators and, importantly, the banks, when looking at transactions, have to think about when they build their systems.

Q909 **Chair:** And think laterally.

Megan Butler: Absolutely.

Q910 **Chair:** We talked about confirmation of payee and the contingent reimbursement model this morning. Is there anything else coming up that is on your radar of developments? FCA?

Megan Butler: We have various pieces of guidance that will not touch on this expressly but will be relevant. We have guidance coming out on vulnerability and how banks should think about it, which will be relevant in this space. That is due later in the summer. That would be the obvious one.

Q911 **Chair:** Anything at the PSR? You mentioned those, too. Is there anything else coming up—anything to be negotiated?

Chris Hemsley: The main focus for us at the moment is ensuring that those big changes bed in properly. Of course, there is always more we can do, but that is our real focus in the next year.

Q912 **Chair:** You are going into the sandbox as well, which I think we are all fans of. Is there anything about economic crime prevention that you are

aware of? You could write to us about that. It would be interesting if the sandbox was being used by anybody, particularly in the economic crime prevention space.

Megan Butler: It is very much in the know-your-customer piece. There is quite a lot of work to see if that can be slightly more on a utility basis. Banks are quite interested in that, because it will theoretically be cheaper. Actually, it should also deliver more effective outcomes, which is more what we would be interested in.

There is definitely exploration of how that process can use more modern technology. As I have said, there are some things coming through around the transaction monitoring piece, which has the capacity to make banks a great deal more effective at spotting potential financial crime. That is a very important space, but even outside the sandbox, there is a great deal of work among regulators, not just here but internationally, on use of technology to shift the dial in our ability to supervise—whether that is around focusing on areas of likely problem and targeting firms that are more likely to be problematic or, more broadly, to help us to test firms' own arrangements. There is a great deal of technology opportunity associated with technology-driven crime.

Q913 **Chair:** I have a final question. Rushanara mentioned the phrase "grossly negligent". We have heard evidence that the term is not being applied consistently. Does the FCA have a view on that? What about Chris and the PSR? Do you think that that phrase should be used in letters to customers, who are not lawyers and are not trained to know what it means, or is it a phrase that really has no place in customer letters? Let's start with the FCA. Is it being applied consistently?

Megan Butler: At this stage, I would say probably not, but something that we are expressly going to look at is how they are treating the customer's experience. If somebody has been tricked into giving away their credentials, we would take an awful lot of convincing that that could amount to gross negligence. That is what we need to see operating in firms, but we need to see them judging each case in a very particular way.

What we really need to avoid is a box-ticking approach from banks. They need to look at the individual and the circumstances and be reasonable about what they can expect to see. We have to remember one key point, if I can make a legal reference: the burden of proof sits with the banks. The presumption is wholly in favour of the victim here, and that is entirely appropriate.

Mark Steward: I got a little confused when you were talking about sticks. If we see banks under the code behaving in a very inconsistent way and making selectively arbitrary decisions about what they will and will not compensate, we will take the view that even though the code is voluntary, banks have publicly signed up to it. If they say that they will follow the code, but then they do not, we might regard that as a very troubling thing. It might give rise to enforcement action if we see significantly poor compliance with the code.

Q914 **Chair:** Chris, does the phrase "gross negligence" have a place in letters to customers?

Chris Hemsley: I should probably record the fact that I agree with what has just been said about the importance of thinking about this case by case. How banks communicate on individual cases is a bit outside my remit; as a private individual, of course I encourage them to communicate them in a clear and transparent way, as you would expect.

Q915 **Chair:** Given all the case law that there is about gross negligence, it may not be quite so clear and transparent.

Chris Hemsley: No. I think the important thing here is the way the code was developed, with the consumer groups involved in its design. This is an area where we will have to keep an eye on cases. The Lending Standards Board is overseeing the code on a day-to-day basis; it plays an important role in that. This is a particular area that we will be keeping a close eye on.

Ultimately, the protection of the Financial Ombudsman Service has not gone away. If people disagree with how the banks have dealt with this, which is quite a tricky issue, they can still go to the financial ombudsman—they do not lose that right.

Chair: Thank you very much indeed for your evidence this morning. You have been very helpful and have made a great contribution towards our inquiry report.