

Treasury Committee

Oral evidence: Economic Crime, HC 940

Tuesday 2 April 2019

Ordered by the House of Commons to be published on 2 April 2019.

[Watch the meeting](#)

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Steve Baker; Colin Clark; Mr Simon Clarke; Charlie Elphicke; Stewart Hosie; Alison McGovern; Catherine McKinnell; John Mann; Wes Streeting.

Questions 722 - 836

Witnesses

I: Mark Tingey, Head of Financial Crime Operations, Metro Bank.

II: Ruth Evans, Chair, Authorised Push Payments Scams Steering Group; Richard Lloyd, Independent Adviser, Authorised Push Payments Scams Steering Group.

Examination of Witness

Witness: Mark Tingey.

Q722 **Chair:** Good morning and thank you very much for being here for the next session in our economic crime inquiry. I am sorry; this is a bigger room than we are used to, even as a big Committee, so we are a long way away, but we will be able to hear you down there. I am going to ask you if you would introduce yourself for the benefit of the tape and for those watching, and then we will get on with the session. Perhaps you could say who you are and the role you hold at Metro Bank.

Mark Tingey: My name is Mark Tingey; I am head of financial crime operations at Metro Bank. My team is responsible for protecting Metro Bank customers, colleagues and the bank as a whole from all aspects of financial crime. I have a fraud team that deals with all the cases that are raised by our customers. We also work proactively in our efforts to prevent fraud. I have an anti-money laundering and AML operations team, which is responsible for the screening and monitoring of our customers and investigations into suspicious activity.

Q723 **Chair:** Thank you for being here for this session today. To start, Metro is a pretty new bank compared to the longer established institutions in the field. Perhaps you could set out Metro Bank's approach to economic crime. Being relatively new, in terms of the structures you have just described, were they designed into the workings of the bank from day one?

Mark Tingey: Yes, absolutely. Financial crime has definitely been a key focus of Metro Bank from day one. I personally joined coming up to five years ago, but previous to my tenure there was a focus on specialism in financial crime. Our approach is very much around protecting customers. Our focus is on protecting customers. If we can protect customers and prevent fraud from happening, fraud losses will take care of themselves. The focus is very much on protecting customers.

Q724 **Chair:** I know you were previously head of fraud and investigations at the Royal Bank of Scotland Group, but, particularly in the last five years, have you seen any change?

Mark Tingey: Yes, absolutely.

Chair: Has it been a change in the prevalence or types of crime?

Mark Tingey: The way that fraud in particular has evolved over the last five to 10 years has been quite significant. Last year I spent some time with one of my teams, which was going out to do some training. They were interested in understanding how fraud had evolved. It was really interesting to look back and see how fraud evolved, going much further back than my tenure.

From what we are seeing currently, the trend is very much around social engineering. What I mean by that is consumers being convinced by



HOUSE OF COMMONS

fraudsters either to give away their security details, which enables fraud to take place, or, in the case of scams, to make the payments themselves. It is really interesting. If you go back 50 or 60 years, we had conmen. The famous Frank Abagnale, from the film *Catch Me If You Can*, started off with fairly basic cheque fraud and ended up conning people into believing that he was a pilot or a surgeon. If you fast-forward to the current day, fraudsters are conmen. They con people into believing that they are who they are not: maybe they are their bank; maybe they are a police officer.

The fraudsters have some very clever techniques, using the technology that is available today. We see social engineering done via email, which is known as phishing; via text, which is known as smishing; and via voice, which is known as vishing. We see all these techniques that fraudsters are using now. If you look back at the investment the whole industry has done over the last five, 10 or 15 years, it has made it harder and harder for fraudsters to access bank systems, so we are seeing a movement: "If I cannot do that, I will get the consumer, the customer, either to do it for me or to give me all their details so I can then access the systems."

Q725 Chair: We will come on to this as well, but, in terms of consumer or customer behaviour, how much of your time, or the bank's time, is spent in equipping customers with the knowledge and the wherewithal to be alert to these types of scams? Have you noticed a change in customer behaviour and knowledge over those five years?

Mark Tingey: Definitely, yes. From a consumer perspective, people are much more aware of fraud. The ongoing education and awareness of consumers is absolutely vital. We fully support and have supported the Take Five campaign through UK Finance, and we have our own campaigns that we do. We have information on our website on how customers can protect themselves and how we protect them. Ongoing education, awareness and keeping people updated on new trends is absolutely vital. As I say, people are more aware today of the threats that are out there than they maybe were five years ago.

Q726 Chair: One of the things we have explored in these sessions is how victims are reimbursed and their success or otherwise. That is what we are going to explore in the second session today about the code. We have heard an example of Metro Bank refusing to reimburse fraud victims, despite them being not being classed as grossly negligent. You might have read it, but Richard Emery, an independent fraud investigator, named Metro Bank as one of the banks he had the most issues with regarding the use of the term "gross negligence". Can you talk us through how Metro applies the term "gross negligence"?

Mark Tingey: Yes, certainly. If I may, first, I would acknowledge the comments that Richard Emery made. The first point I would make there is that this was based on a very small sample size, in terms of the number of cases that he was working on. Specifically looking at gross



HOUSE OF COMMONS

negligence, it is in the PSR regulations. Unfortunately, there is no definition and very little case law in terms of gross negligence.

The way we approach every single one of our cases is that we investigate all our cases. We gather all the information that we can from the customer and from our own investigation to understand exactly what has happened. No two cases are ever the same. We do that thorough investigation and then we make an assessment, based on gathering all that information, as to whether we consider, ultimately, this is something where there was no way the customer could have done anything, and therefore they would be due a refund, which happens in the vast majority of cases. If we identify a case where we believe the customer, under the terms of the regulations, has been what we consider grossly negligent, we will decline the claim.

In all cases, we always give the customer the opportunity to challenge that decision. That will be reviewed independently from my team. It will generally be reviewed through our customer relations team. There will be an independent review. Ultimately, if the outcome of that is that we still believe the decision is to decline, we always give the customer the option to take that to the Financial Ombudsman for a final adjudication on the decision.

Q727 **Chair:** You said there that you fully refund in the vast majority of cases. Do you have a percentage of how many cases get fully refunded?

Mark Tingey: Yes. We refund in the region of 95% of cases.

Q728 **Chair:** How many claims have been rejected? I do not know whether you do it on a calendar-year or a financial-year basis. In the last year for which you have complete figures, how many have been rejected?

Mark Tingey: I do not have that specific number, but I am happy to come back and provide that information to you.

Q729 **Chair:** On what grounds would you reject reimbursement? Is it the gross negligence test? Do you say to people, "We think you have been grossly negligent", or is it put to them in a different way?

Mark Tingey: It is aligned to gross negligence. We do not just say to a customer, "We are declining it because you have been grossly negligent". In all cases, we fully explain to the customer our rationale and our reasons for declining it so they are very clear. That enables them to come back and potentially challenge us, to say, "Actually, there is some further information". We want them to be clear to the ombudsman as well, when it gets the case, so it can see the reasons we have declined and can focus its investigation on those specific reasons.

Q730 **Chair:** I am sorry to push you on this, but would you use the phrase "grossly negligent" in a letter back to a customer? Would you, as a standard, make sure that phrase is in the letter?



HOUSE OF COMMONS

Mark Tingey: Generally not, no. We focus on the specific, actual reasons why, as opposed to saying “grossly negligent”, but it is aligned to what we consider to be grossly negligent, in line with the regulations.

Q731 **Chair:** That is a discussion internally that you have had: “This is how we measure gross negligence”.

Mark Tingey: Yes. We would look at it on a case-by-case basis. As I say, no two cases are the same. We have an escalation process as well, and we will review. For a particularly complex case, for example, we have a forum where we will meet and we will consider all of the aspects of the case. We will involve other colleagues, for example, from our customer relations team so we have not just the fraud angle. We consider all the aspects of the case and then determine whether we believe we should refund, or whether we believe the customer is liable.

Q732 **Chair:** Is the phrase “grossly negligent” something that you think customers would react badly to? It is a phrase that people might not understand; they might almost think that it is a rude phrase.

Mark Tingey: Yes, the main issue is that, as I say, there is no clear definition of what it is. If I received a letter that just said, “You have been grossly negligent”, my first question would be to ask, “What have I done?” Explaining the reasons makes them clearer to the customer.

Q733 **Mr Baker:** Metro Bank has a new banking model with stores rather than branches, I understand. Customers can walk in without an appointment, with no bank account, and walk out with a bank account and, indeed, a card printed on the spot. It all sounds brilliant for consumers, but however does it work, in terms of preventing economic crime?

Mark Tingey: You are absolutely right. In that model, you can walk into one of our stores, seven days a week, open an account and walk out after 20 or 30 minutes with your account open, your card, your login for online banking and everything you need. We use sophisticated technology in all our stores and in our online account opening, which we launched last year. It checks the ID—for example, the passports and driving licences that customers provide—and enables us to validate that the ID is genuine. We are very confident that the accounts we open are being opened with genuine ID and the person holding that ID is the person opening the account. The volume of impersonation fraud that we see through our stores in our current account opening is extremely low.

Q734 **Mr Baker:** You are using technology to check the validity of the ID, not people.

Mark Tingey: We use technology to check the validity of the ID. Our store colleagues will then check to ensure the photograph on the ID matches the customer who is in front of them. As part of our account opening, we then maintain a photograph of the customer on our system, which we use to authenticate them. If they come into store once they



HOUSE OF COMMONS

have their account, we can use that as an identification method to ensure that we are serving the correct customer.

Q735 Mr Baker: I am just looking at the list of proofs of identity that you accept, which include a valid UK, EEA or Swiss passport, a UK full or provisional photocard driving licence and a valid EU member state ID photocard. This seems a very wide range potentially, if it is any EU national ID photocard. They have varying degrees of authenticity, do they not? Tell me a bit more about this technology and to what extent you can rely on it.

Mark Tingey: You are absolutely correct in terms of the ID. We are aligning to the regulation in opening accounts as well. Our account opening requirements are aligned to the regulation that is laid down. The technology we use is very similar to the technology being used at airports, at passport control for example, where you put your passport in and it validates that it is genuine. The technology we use scans the ID document and then, by looking at various aspects of it, is able to validate for all countries that it is a genuine document. As I say, it is then reliant on our colleagues to ensure the photograph matches with the individual and it is not somebody else trying to use it.

Q736 Mr Baker: Is this a proprietary technology of your own or is it something you have bought?

Mark Tingey: No, it is something we have purchased.

Mr Baker: Would you mind just telling us the name of the vendor so we can perhaps do some research around it?

Mark Tingey: The technology we use in-store is called IDscan and the solution we use on our online banking is called Jumio.

Q737 Mr Baker: Is in-store card printing more or less secure than the traditional method?

Mark Tingey: It is as secure. We have controls in place for the cards themselves. We have specific controls in place for the customer coming in. As I mentioned, we keep photographs of the customer so we are able to identify customers. As you say, if you acquire a new card, you can come into store seven days a week and have that card with you in 10 or 15 minutes. From a customer service perspective, it is a fantastic tool that we have.

Q738 Mr Baker: Some of the documents that you require for proof of address need to be originals and not printouts from the internet, but there is of course a move to paperless and online only. All of us will know that there are penalties if you do not move over to paperless. Where does this leave your customers, as the world moves to paperless?

Mark Tingey: We are continually evolving and continually reviewing the documentation we receive and how we can validate those documents. You are absolutely right: personally, I do most things online now and I



HOUSE OF COMMONS

very seldom get paper statements. We are continually reviewing that to ensure the documents we get are genuine. We do checks with credit reference companies. If the customer has that profile, that is one way we would validate that. If they do not have that file, we rely on documents being provided.

Q739 Mr Baker: That is not quite the question I was asking; forgive me. As the world becomes more paperless, your customers—in fact, any bank's customers—are going to become less able to provide original documents from their service provider. How will you cope with that phenomenon? People will have less opportunity to bring you original documents.

Mark Tingey: As I say, we need to continually evolve in how we obtain those documents, and look at the best way we can obtain them securely, ensuring that they have not been doctored in any way. I cannot specifically answer that question now but, in terms of that continual involvement, we will continue to look at that and ensure we maintain that balance between maintaining our customer service proposition and having the right fraud controls in place.

Q740 Mr Baker: Do you have any analysis on what types of document are more likely to be subject to fraud?

Mark Tingey: I do not have that, I am afraid.

Q741 Mr Baker: Is it work that you could do?

Mark Tingey: We could certainly go away and look at the accounts that we have, to see whether there are any particular trends in terms of that documentation.

Mr Baker: If it is not too much trouble, I would be grateful for that.

Mark Tingey: We would be happy to go away and look into that.

Q742 Mr Baker: You have mentioned that you are using technology to check these documents, and you said that staff are checking that the photos match. What additional training do staff need in order to ensure the technology does the job that it ought?

Mark Tingey: All our colleagues joining the bank have specific fraud training. My team provides fraud training as part of our overall induction plan. All colleagues go through that. All our colleagues also do fraud training twice a year through our relearning models. We have some specific training that we will provide to our colleagues who are opening accounts. It gives them advice on the sorts of things to look for and how to compare a photo. There are some quite clever things that you can look at when you are looking at a photo, like the positioning of the ears against the nose. There are some tips we can give.

Sometimes the photo could be up to 10 years old, if it is a passport. It is about being able to give them those key features and help them understand. If we were in a situation where it was a particularly old photo



HOUSE OF COMMONS

on the document and we were not able to validate, we would ask the customer whether they had any additional ID that we could take to help us validate and authenticate the ID they were providing.

Charlie Elphicke: Good morning. Can you hear me okay?

Mark Tinge: I can, thank you.

Q743 **Charlie Elphicke:** That is great. I just wanted to check that I did not need to use a loud hailer. Forgive me while I adjust my telescope. How is Metro's implementation of confirmation of payee progressing?

Mark Tinge: Confirmation of payee, as you will probably be aware, is the industry's solution, looking at the matching of payees. We are aligned with the industry in where we are with that. It is a significant development for us, as it is for all the banks, in terms of both updating the payment systems and the development internally. Currently, the industry position is looking at an implementation of confirmation of payee in early 2020. We are currently mobilising a project for that at the moment, and we are aligning ourselves to that implementation.

Q744 **Charlie Elphicke:** To what extent does the system require all its participants to be ready before it can be activated?

Mark Tinge: The more participants there are, the more successful it is going to be. Ultimately, we need all the banks involved in that to ensure it is fully functional, so we are getting the messages to and from wherever the payments are going. That includes new entrants into the market.

Q745 **Charlie Elphicke:** Do you think it will work? Do you think it will put a stop to all these crooks who have been ripping people off for years and years?

Mark Tinge: Ultimately, the proof will be once we actually implement it. The principle is there. The challenge with it is around the matching and how good the matching can be. One of the challenges at the moment is that there is a limited number of characters that you can put into a payee when you are creating a new payment. That is one of the changes being made to the payment system: to make it so that you can put more information in there.

We are conscious that people use different names. Some people might use their second name instead of their first name; some people use surnames for first names. Particularly for businesses, they could have a holding company and a trading name. The key is really going to be the success on the matching criteria to ensure we do not create too many, as we would refer to them, false positives. For payments that are correct, we do not want to put too much grit into the payment system and be challenging payments that do not need to be challenged. If it works, from a scams perspective it should have a positive impact on mandate-redirection frauds, which tend to be the higher value frauds.



Q746 Charlie Elphicke: Let me give you an example. Let us say I go and buy a Reliant Robin from Trotters Independent Traders and I spell "independent" with an "a". What will the effect be? Will it then chuck out the transfer altogether or will it flag it up? What happens?

Mark Tinge: That is what we are working on in terms of technology now. I mentioned the matching. We need a system that will go, "That is an obvious spelling mistake, so we are not going to flag that up". Otherwise, the danger is that there will be so many payments that are flagged up. It is about being able to identify the ones that are very clearly a mismatch, as opposed to something that someone has just mis-keyed or transposed some digits. That is going to come down to that matching. That is key.

Q747 Charlie Elphicke: I guess the question is this. If I spell "independent" properly, with an "e", and it all goes through, that is fine. If I spell it with an "a", will it be flagged up so that someone at the bank looks at it and thinks, "Yes, that is meant to be that", or will it use machine learning and be done by AI in some way?

Mark Tinge: At the moment, because it is very early on in that development, it is difficult to answer that question. The idea is that, particularly if a customer is setting up a payment themselves through their online banking or mobile banking, it will give them a warning. It needs to be sophisticated enough to identify a genuine mistake versus a clear fraud.

Q748 Charlie Elphicke: With confirmation of payee, is there a risk that you will get moved from what you might call vanilla push-payment frauds to what you might call impersonation fraud?

Mark Tinge: As I mentioned earlier, the key trend and threat we see at the moment is around social engineering. It is around frauds as convincing customers. The key challenge is going to be whether the fraudsters can convince a customer, "Even though it is a completely different name, just carry on. That is absolutely fine". That social engineering threat will remain. I mentioned the education of customers and making them aware. We have to get the key message out to say, "Irrespective of what someone is telling you, if that does not match, do not make the payment". It comes back to Take Five. Do some further inquiries. Do not rush. Just make some further inquiries before you make that payment. It is a warning system to a customer, to tell them, "Something is not right here. Take some time to go away and do a bit more research".

Q749 Charlie Elphicke: Looking at flagging, how do you respond when it becomes apparent that there is a cluster of fraudulent accounts located in one bank?

Mark Tinge: To clarify, this is in terms of the beneficiary accounts that the moneys are going to. Looking at that, we refer to accounts that receive beneficiary fraud as mule accounts. We are employing technology



HOUSE OF COMMONS

that helps us identify key attributes from that account that would indicate there are other accounts. There is an industry pilot that we are also involved in, which is being run by Vocalink, called the Mule Insights Tactical Solution. That is helping to proactively identify prospective mules based on activity from other accounts. Where we identify those, we will take action to investigate. If we believe they are being used, have been used or plan to be used, we will look to close those accounts.

Q750 Charlie Elphicke: What interrelationship do you have with the police? Do you have regular communication with them? Do you find it effective or is it byzantine, confusing, muddled and chaotic?

Mark Tinge: Where we have cases that are taken on by law enforcement, the service we get and the outcomes we see are excellent. We work very closely with the City of London and the Met Police in particular. As I say, for the cases they take on, I cannot praise enough the support that they give. The challenge is the wider resource piece, in terms of the number of cases that they are able to take on.

Q751 Charlie Elphicke: When you say "the cases they take on", what percentage of cases do they take on? For what percentage of cases do they say, "That is too difficult. We are just going to bin that"?

Mark Tinge: I do not have specific numbers, but the percentage is low in terms of the take-up.

Q752 Charlie Elphicke: It is low. Have you heard of an organisation called Action Fraud? Are you aware of what it does?

Mark Tinge: I have. I am aware of Action Fraud.

Q753 Charlie Elphicke: What does it do?

Mark Tinge: Action Fraud is there for a consumer to report fraud, all aspects and all different types of fraud, where they have been a victim. Where a customer has been a victim of fraud, we would actively encourage them, first, to report it to their bank so we can take action. Action Fraud maintains the data and does analysis from the point of view of all the information it gets, to help provide intelligence about future threats.

Q754 Charlie Elphicke: My constituents in Dover are quite sceptical of Action Fraud. They call it "Inaction Fraud". Is that fair? Is there an issue there?

Mark Tinge: From the point of view of the analysis it does, it is effective. The challenge comes from a point of view of law enforcement and the resource availability to take cases forward.

Q755 Charlie Elphicke: Finally, we have a tradition in this country where you have an economic crime case that is taken on by, say, Sussex Police or the City of London Police, who may not handle it very well. There are different police forces all over the place; you have the whole thing with Action Fraud, which does not seem to work terribly well. Is it now time to



HOUSE OF COMMONS

have a proper, centralised economic crime command, an economic crime police force that has a concentration of expertise, to go after these crooks, nail them and put a stop to this properly, rather than allowing it all to continue growing, as it seems to be?

Mark Tingey: It would be excellent if we could get that. The City of London police are the experts in fraud. I know they co-ordinate a lot of that fraud work, but having that dedicated resource would be a positive way forward.

Q756 **Colin Clark**: Could you outline how Metro Bank is able to identify patterns of fraud affecting consumers?

Mark Tingey: Yes, certainly. We employ different sorts of technology in identifying fraud. We employ what we refer to as a layered approach to fraud prevention. For example, we will have the up-front controls, which are very well known, around PINs and passwords. We have some step-up controls around two-factor authentication. We send one-time passcodes to customers, for example.

We also employ tools behind the schemes to actively identify themes and trends that can identify suspicious behaviour or activity, which we would then be able to act upon. That may result in us either asking the customer for additional authentication or, if it was a particularly high-risk transaction, declining that transaction and then contacting the customer.

Q757 **Colin Clark**: Compared to the traditional models in banks, would it be fair to say that you would consider yourselves more nimble and more technology dependent?

Mark Tingey: I definitely believe we are more agile. Because of our size, we are able to respond very quickly. If I may give an example, last year there were a number of large data compromises: British Airways and Ticketmaster, to name two. UK Finance does a great job in working to gather all the information of the consumers whose details have been compromised.

What happens when we receive that information? Let me give you one example from last year. We had some customers whose card details had also been compromised, as well as their personal details. We were able to very quickly contact all those customers, cancel the card that was at risk and offer them a new card. Having our stores, they were able to come in, if they could. They could come into the stores upon receipt of that letter and get their card within 10 or 15 minutes. If they could not do that, we were able to send them out a new card. We were able to respond really quickly to that threat and to protect those customers from potentially fraudulent activity on their account.

Q758 **Colin Clark**: Is the big difference now that real-time payment requires fast identification of fraudulent transactions? Using historical data is no longer sufficient, with the banking system we have.



HOUSE OF COMMONS

Mark Tinge: With faster payments, the speed at which payments move is absolutely challenging, but the technology that we are using to identify that suspicious activity helps us, as I say, either to stop those payments going out or to get additional authentication from the customer to validate whether that payment is genuine.

Q759 **Colin Clark:** Is the banking industry putting convenience in front of security? It is all very well saying that consumers want greater convenience. I understand that. All of us sitting here probably do electronic banking; they are probably doing it right now as they use their phones. It would be fair to say you are offering convenience, but is the banking industry really keeping the public abreast of the security risks? Have we jumped ahead of the security?

Mark Tinge: Speaking from a Metro Bank perspective, maintaining that balance between customer service and fraud protection is absolutely key. We are focused on that all the time. Getting that balance right can be challenging. As you say, if you go too far one way, you end up with more fraud; if you go too far the other way, we end up with a lot of genuine customers who are inconvenienced by the additional controls that are in place. We are continually looking at striking that balance.

We invested around £10 million last year in fraud prevention across different technologies and people. We have a project that we are running at the moment looking across all our channels. From an authentication perspective, it is looking at how we authenticate customers. We are looking to provide an excellent service, but also to provide excellent protection.

Q760 **Colin Clark:** You mentioned a figure of £10 million. Is there a figure for how much people were defrauded of last year, even at Metro Bank? Do you know? Is there a figure?

Mark Tinge: The industry figures were out last week, which showed £845 million across the industry. Looking at it from another point of view, £1.2 billion was prevented as well. Two pounds in every three was prevented by the banking industry, so there is a huge investment across the industry. That continually evolves.

Q761 **Colin Clark:** If there was an armed robbery for £845 million, it would be in the front of the paper, would it not? This is the issue that my colleague was just asking about. It seems that online financial crime is just not significant. I cannot remember the quote, but if it does not bang, make a noise or bleed, people do not seem to pay attention. Is that the problem? Is that the difference in financial crime?

Mark Tinge: You are correct. You are absolutely right in that respect. It comes back to the point made earlier around the profile from the point of view of law enforcement and the amount of cases that are taken forward. It does not have the same profile, as you say, as it would if that money had gone through a bank robbery.



HOUSE OF COMMONS

Q762 **Colin Clark:** I worry about the law enforcement, because I think we are doing it the wrong way round: the horse has already bolted and the stable door is wide open. On that matter, what do you believe will be the impact of open banking, which I had to look up, on consumer vulnerability to economic crime? This is the idea about application programming interfaces, which depend massively on third parties. For the sake of convenience, it seems terrifying.

Mark Tinge: This is another example of technologies creating additional risk. Open banking will create new risks. From our perspective, I know my colleagues across the industry are working extremely hard to ensure we manage those risks and have the right controls in place so that customers who actively use open banking can do it in a convenient but also a very safe way.

Q763 **Colin Clark:** It is the "safe" that worries me. It sounds to me like we are giving third parties the keys to the safe. Again, if this was physical, we would be deeply uncomfortable if we thought that application programming interfaces, which can be independent third parties, also had keys to the safe at Metro Bank. I am sure there is not a big safe at Metro Bank.

Mark Tinge: Aligned to open banking is the regulation, for example, around PSD2, with secure customer authentication. We are ensuring that we align the two so we have the controls and we can provide the convenience. It comes back to the point around getting a balance between what customers want from customer service and ensuring there is adequate protection in place.

Colin Clark: I hope so.

Q764 **Rushanara Ali:** I have some further questions on fraud prevention. I wanted to pick up, first of all, the question about policing. You mentioned the City of London Police and their role. Financial contributions get made, presumably, through the Corporation of London process as well. Do you know whether the banking sector makes any additional contribution towards investigating fraud where the police are involved? Do you expect that to come from the general policing budget?

Mark Tinge: Within the City of London Police there is a specific department called DCPCU. That is fully funded by the banking industry.

Q765 **Rushanara Ali:** Any crime committed anywhere in the country that is fraud would be investigated by them, would it?

Mark Tinge: We report them into the DCPCU. I do not know how many they pick up. I do not have the details to hand, but they have specific focus areas that they will be looking at each year.

Q766 **Rushanara Ali:** My question is this. If a fraud was committed in another part of the country, you relayed that to the police and the police needed to be involved, who would investigate that? Which police service would



HOUSE OF COMMONS

investigate it? Would it be that unit in the City of London Police or would you expect the police in that other region to deal with it?

Mark Tingey: Where we have a case, the process we would generally follow is that we would refer it to the DCPCU in the first instance. I am aware of instances where they have then liaised with the relevant regional force.

Q767 **Rushanara Ali**: Those original forces do not have a separate financial contribution made by the banking sector to investigate fraud that has been committed within the banking sector, do they?

Mark Tingey: They do not, no. It is specifically for that.

Q768 **Rushanara Ali**: To give you a parallel example, my local authority is having to co-finance for extra police officers out of council tax funding because of the police cuts. Given that you are relying on other forces to investigate banking fraud, why are you not making a contribution like that to bolster the police service, in response to the fact that you are using police resources because of things going wrong in terms of fraud in the banking sector? Local authorities are having to find public funding elsewhere to compensate for the funding cuts in the police service. Is that something you would consider doing as the banking sector? I know you cannot speak for the entire banking sector, but you have a responsibility here. You are involved in some of the discussions with the wider sector. What do you think of that?

Mark Tingey: As you say, I cannot speak for the wider banking sector.

Q769 **Rushanara Ali**: How about for your own bank? Is it fair for the public to expect your bank to make a contribution to police resources where that bill is not being picked up within the provision that is being made within the City of London Police?

Mark Tingey: We would need to go away and consider that.

Q770 **Rushanara Ali**: Can you understand the unfairness of what is going on here?

Chair: Let Mr Tinge answer the question.

Rushanara Ali: I just wanted to explain the point.

Mark Tingey: The fact that the banking industry funds that section within the City of London Police is fairly unique to our industry. I am not aware of other industries that would do that. Given that we do it and have done for a number of years, we already have that focus. In terms of whether we would be able to take that wider, I cannot comment on that at the moment.

Q771 **Rushanara Ali**: The reason I raise this point is that we have heard reports that, in terms of banking fraud generally and these sorts of fraud cases, the police are struggling and it is not being prioritised as much as other crimes, like violent crime, which is understandable. How are the



public meant to have confidence that, when the police are required to intervene, particularly outside London, where you need co-operation from other police forces, the investigations are going to take place, unless they are properly resourced? That is the point I would be very keen for you to take away and feed into the wider industry. It is of concern, and it is not going to inspire confidence in the ability of the banking sector and the police service to deal with it, even if there are specific cases where people are doing the best job they can, as you mentioned earlier.

Turning to the recent Which? and SureCloud test, it showed that Metro Bank was the worst performer in online security among banks. The test showed that barely half of the security features met Which?'s standards. Can you give some commentary to that conclusion?

Mark Tingeey: Yes, certainly. At the time, we responded to the Which? survey. There are a few points I would make in that space. We acknowledge the findings of the report, but it does not take into account, as I touched on earlier, the layered approach that we apply. There are additional controls sitting behind the scenes that give us confidence in the controls we have in place. As I mentioned, this is something we are continually looking to evolve. We are currently looking at our authentication model, how we authenticate customers and how we can make it as secure as possible while making it the best possible customer proposition. It is very high on our agenda at the moment. It is something we will continually look to improve.

Q772 **Rushanara Ali:** Is there a timeframe you are looking at to try to address those concerns and priorities?

Mark Tingeey: We are confident in terms of what we have. The project I am referring to is over 12 to 18 months. It is a significant development, but we will look to implement changes during that period.

Q773 **Rushanara Ali:** Referring back to the newspaper reports in February that Metro Bank had been targeted by hackers and they were able to set up online payments by taking control of mobile phone numbers, can you say a bit more about the interaction with the phone companies, what they are doing and how much co-operation there is with the sector in trying to deal with that dimension?

Mark Tingeey: Yes, certainly. If I can comment specifically on the piece you are referring to, the first point I would like to make is that it was not a cyber-attack against Metro Bank. If I could explain, as I mentioned earlier, we investigate all our fraud cases. Through a case we were investigating, we identified that the text message we had sent to a customer with their one-time pass code for their authentication had not been received by them. We work very closely, as a bank and as an industry, with the telecommunications industry. We were liaising with the mobile operator for that specific customer. Through those discussions, it emerged that there was a potential compromise of what is known as SS7, which is the mobile network operators' platform.



Following that conversation, through support with external stakeholders, we were able very quickly to get other banks from across the industry and other telecommunications companies to look into what the issue was and to identify whether it went further. The mobile network operators took that away and fixed the specific issue. From our perspective, we had a small number of customers, 11 customers, who were impacted by that, and those customers who lost money as a result of fraud were all refunded as a result of that. As an industry, we work very closely with telecommunications companies on a number of aspects.

Q774 Rushanara Ali: Do you feel, not just from your own perspective but more widely, because of what you have done and what has arisen, that consumers can be much more confident that they are not going to face issues like this in the future?

Mark Tingey: We have not seen any further cases of that, so we are very confident that that specific issue has been fixed. Around using SMS in particular, we are aware that there are risks with that. It comes back to the balance between customer convenience and security. That is also a key part of the programme in which we are looking at alternatives to move away from our reliance on SMS.

Q775 Mr Clarke: Having heard all about risk, I will move us on to derisking. Of course, here the question becomes how we avoid derisking in such a way that we end up throwing the baby out with the bathwater. We have heard concerns about whole sectors or groups of people being ruled out of bounds by the sector because the risks are just too great. How does the Metro Bank approach the issue of derisking?

Mark Tingey: First, in terms of our approach, Metro Bank is very much a UK community bank focused on providing services to retail and, in particular, our small and medium enterprise portfolio. We offer basic banking products—loans, deposits, current accounts, asset finance—to all UK-based customers through our stores. That is our market. From the point of view of derisking, we assess all the customers who join us. If a customer joins us who is considered to be of a higher risk, those risks will be assessed and we will compare them to the controls we have in place. If they are outside our documented risk appetite, we will not proceed with opening that account.

Q776 Mr Clarke: In terms of what factors influence that risk appetite, are there particular sectors or nationalities? I am just trying to understand the framework within which you make those decisions.

Mark Tingey: There are a number of different factors that we would consider. For example, looking at high-risk countries and prohibited countries is a key factor that we would consider. We would look at all the different aspects. If it was a company, we would look at the company, the individuals behind the company and the ultimate business owner of the company, to understand whether any particular red flags came up



HOUSE OF COMMONS

from that risk perspective, so we could undertake that full risk assessment.

Q777 Mr Clarke: Who defines which countries are deemed high risk? I can quite appreciate that obvious examples come to mind, but what is the exhaustive list or the illustrative list? Who sets that?

Mark Tingey: It is specific from a regulatory perspective. A lot of that is set through regulation in terms of specific countries that have different sanctions against them, for example. We would consider them to be high risk. That framework is there for the bank to look at and assess which countries it feels are within its risk appetite and which ones are not.

Q778 Mr Clarke: How many individuals, and indeed how many businesses, did Metro Bank decline services to last year?

Mark Tingey: I am afraid I do not have that data to hand, but I would be more than happy to take that away and provide that information back to you.

Chair: Would you let us have that?

Q779 Mr Clarke: Yes, that would be helpful. Thank you very much. In terms of individuals who do fall foul of the risk appetite issue, what right of appeal exists? What information are they given regarding their options at that point?

Mark Tingey: Through the whole account opening process, the customers will be kept informed and provided with a rationale for why we are not going ahead with the particular account. We have a process whereby they can raise a complaint, and that decision will be considered. It will go through that due process. There is an escalation process that they can go to.

Q780 Mr Clarke: In terms of good governance, on the basis of my whole three years as an MP, or two and a half years, it seems to me that the absolute No. 1 objective needs to be avoiding perverse incentives in the legislation you create. Are the anti-money laundering rules fit for purpose? Are they providing a perverse incentive that means you are effectively forcing people out by making it too risky for the banks to operate and take on these customers?

Mark Tingey: From the point of view of the regulator, in 2017 we saw a significant uplift in legislative standards through the anti-money laundering regulations that were implemented. As a bank, we welcomed those regulations. There are further enhancements coming with the fifth anti-money laundering directive. From what we have seen of the provisions that are coming out of that, there is information in there that we would welcome to support the industry and to support customers. Looking at it particularly in terms of the SAR regime, there are well-documented inefficiencies within that process that are being analysed through the SAR reform. The short-term improvements we are



HOUSE OF COMMONS

seeing coming out of that are encouraging, and we are looking forward to the more strategic review of that.

Q781 **Mr Clarke:** When you make a mistake on your side with customer due diligence, what happens? What are the consequences that flow from that?

Mark Tinge: It would really depend on the circumstance. From the risk perspective, the risk is that the account would go on and commit some form of financial crime, so we potentially will end up having a SAR investigation. The wider implications would be, for example, if an account was opened for a sanctioned individual that had specific ramifications on the bank from a regulatory perspective. The wider risk piece is around having those accounts that could ultimately become vehicles for money laundering.

Q782 **Mr Clarke:** On the flip side of that, have any banks been held to account and criticised by the regulators for being unduly risk averse and shutting too many people out of financial services?

Mark Tinge: I do not have that information, I am afraid.

Q783 **Catherine McKinnell:** We heard evidence from Santander and Nationwide previously about the issue of money mules. As a challenger bank, do you find this phenomenon of money mules to be a challenge for you as well?

Mark Tinge: Absolutely, yes. It is an industry challenge, from the point of view of our accounts. What we see, which again mirrors the industry, is that mule accounts tend to fall into two categories. There are accounts that are specifically opened purely to receive the funds and pass them on, but what we see in around 70% of cases is existing accounts that may have run perfectly normally. Coming back to the social engineering piece, that accountholder has been coerced into allowing funds to be put into their account and moved those funds on.

What we see, which again aligns to the information we have heard back from industry, is that around 50% of the mule accounts that we identify are for under-24s. It is prevalent in the lower age groups. Particularly on social media—Facebook is an example—mule recruiters are very active in encouraging individuals to make money quickly, which ultimately ends up with them being a mule account.

Q784 **Catherine McKinnell:** I am a Newcastle MP, and we are a big student city. As much as I would not want to denigrate students in any way, it has been identified as a target group where they may geographically move for a year or move on from their studies. You put it as “coerced”, but there are incentives to handing over your account for somebody else to use. This is a criminal offence, so what are you doing as an industry to make sure people realise the risks? It might be helpful for you to set out what those risks are to individuals who are thinking about doing this.



HOUSE OF COMMONS

Mark Tingey: Ultimately, accepting proceeds of crime and moving proceeds of crime from your account is a crime in itself, so it is a criminal offence to do that. We do work in our communities. We did some work recently with some under-16s where we particularly focused on this issue. Is saying it is a criminal offence a deterrent? Will they be caught? That will be their comeback. The other implication is that, wherever any mule accounts are identified, they are loaded to the Cifas database. That means, going forward, they will not be able to open a bank account or get a mortgage.

We have identified that, if you say to a 17 year-old, "You will not be able to get a current account or a mortgage", it is not a particular disincentive. The key one is to tell them that they will not be able to get a mobile phone contract. It is about identifying the key points for that particular demographic that will get them to sit up, listen and understand the implications of either actively or passively allowing this activity to take place.

Q785 Catherine McKinnell: It is interesting to hear about the work that you are doing with 16 year-olds. Is enough being done in schools to educate young people about a crime they probably have not given any thought to, given that they probably will not really have a bank account or be regularly using a bank account at that age? Is it important to get that awareness before they become students, leave home and then find themselves potentially at risk?

Mark Tingey: Yes, absolutely. Educating schoolchildren at that age as to the implications, particularly around the mule activity, is really important. We have done some activity in the community specifically focused on that. UK Finance has also done some targeted activity focused on mules. The more we can do, the better.

We have something we call Money Zone, where we go into local schools to teach the kids about banking in general. For key stage 3, we are starting to build in and talk about fraud, particularly social engineering and the mules. It is really important to do more collectively in schools to educate, generally around banking and finance, and specifically around the risks.

Q786 Catherine McKinnell: Is it possible to inadvertently become a money mule or is it always something that people are conscious of?

Mark Tingey: We have seen examples where it is inadvertent. We have seen examples where someone sends someone a payment and then says, "I am really sorry. I sent that to you by mistake. Can you send it here?" They actually do not realise where that money has come from. You see signs on traffic lights saying, "Work from home". Some of those can be mule herders trying to get people. It is possible that people are becoming mules without realising it.

Q787 Catherine McKinnell: It would be interesting to know how many



HOUSE OF COMMONS

accounts you have closed in the last year because of suspicions or evidence that they are money mules. Have you found yourselves not able to close accounts even though you may have suspicions about them? Does the framework support you in clamping down on this?

Mark Tingey: Where we identify a mule and we have evidence of confirmed fraud—so it has definitely been a mule account—we absolutely close accounts down and load them onto Cifas. We do around 200 a month of those. There are situations where, as you say, it is more of a suspicion. That makes it more difficult, because we do not have that evidence. Those will be cases that we will investigate. Depending on how strong the suspicion was, we may take the decision that we are going to exit, or there may not be sufficient evidence to warrant doing that.

Q788 **Catherine McKinnell:** In one sense, there should be no differentiation, because it is a crime. On the other hand, there are people who are very consciously doing this, and you are able to identify those accounts, particularly where they have made a fraudulent transaction. Where people, possibly through lack of education, lack of awareness or vulnerability, are being targeted, presumably that is harder for you to identify and take pre-emptive action on before they have committed a crime.

Mark Tingey: Yes, absolutely.

Q789 **Catherine McKinnell:** Is there anything more that we could do to support that?

Mark Tingey: Going back to your suggestion, particularly around the whole education piece, schools are really important. As I say, we are definitely seeing a very high percentage of young people being targeted, but it is not just young people. If you go back to the point around incentives, if someone is in financial difficulties and someone is offering them a few hundred pounds just to move some money through their account, they are going to be vulnerable to that. They are not necessarily vulnerable per se, but they are vulnerable to that attempt. Some more targeted information would be excellent, just really helping people understand. Ultimately, if we can stop the mules, the fraudsters have nowhere to send the money to. It helps to prevent the fraud in the first place too.

Chair: Thank you very much indeed. That has been very helpful. We are very grateful to you for your evidence and your time this morning. It is much appreciated. Mr Tingey, thank you very much.

Examination of Witnesses

Witnesses: Ruth Evans and Richard Lloyd.

Q790 **Chair:** Welcome very much to our second panel of this morning, for a continuation of the economic crime inquiry. I am going to ask our



HOUSE OF COMMONS

panellists to introduce themselves and then we will get straight on with it.

Ruth Evans: Hello, I am Ruth Evans and I chair the APP Scams Steering Group.

Richard Lloyd: Good morning. I am Richard Lloyd. Until the day before yesterday, I was the independent adviser to the APP Scams Steering Group.

Q791 **Chair:** Thank you very much. Starting off on the setting up of the contingent reimbursement model, the steering group was obviously set up in February last year. The code comes into effect from 28 May this year. There had been an expectation that the code would be introduced by September 2018. Can you perhaps explain the reason for the delay? What were the main obstacles that you had to overcome?

Ruth Evans: The steering group first met in April last year, almost a year ago to the day, on 5 April. The PSR announced the steering group but we had to ensure that we could appoint the members and get the meeting in the diary. The first meeting was in April and, actually, it was a pretty speedy working period of April to September, by which time we got the code out for consultation. It was quite an intense period of work by the steering group.

Could I just pay tribute to the steering group? It is made up of an equal number of consumers and payment service providers. I do not think this has been done before. It was an ambitious endeavour and one that has paid off, but it was not the easiest of challenges to deliver.

Q792 **Chair:** Why was that? Was it due to people coming with different perspectives?

Ruth Evans: Yes, exactly. There were different perspectives in the room, but the steering group found its way to working together and creating a consensus consultation that went out in September. Once that consultation went out, we gave a very short period of time for responses to come back from the industry and other stakeholders. We then examined those in November and December. Those took time. We got 50-plus responses, some of which were very thoughtful and needed a lot of consideration. As a result of that, we published the code a month late. We had hoped to get it out in January, and that is what we had always been committed to within our timetables set by the PSR. We were actually a month late in the end.

Q793 **Mr Baker:** Since we are discussing payment service providers, I should remind the Committee of my interest in Glint Pay. Could you remind us which banks and payment service providers have signed up to the code so far?

Ruth Evans: Those that have said they will be signatories to the code when it is published on 28 May are those on our steering group. There will be a substantial number more, but the initial signatories are those of



HOUSE OF COMMONS

the steering group. Those are Barclays, Santander, which is not on the steering group but has committed, Lloyds, Metro, HSBC, RBS and Nationwide, which again is not on the steering group but has committed to sign up in the first instance. We will have many more PSPs signing up.

Q794 **Mr Baker:** Has anybody been notably reluctant to sign up?

Ruth Evans: No, not to my knowledge. The PISPs are going to have particular challenges of their own, but though authorised they have not yet started business and will do so in September. They have particular needs.

Q795 **Mr Baker:** When I went through the code earlier, it seemed to me that there are a couple of areas where some considerable complexity could be possible. I am just trying to find one now. For example, "Firms should establish transactional data and customer behaviour analytics incorporating, where appropriate, the use of fraud data and typologies to identify payments that are at higher risk of being an APP scam". That feels like quite an expensive thing to do for perhaps a smaller bank. I wonder if that was an impediment to anyone signing up.

Richard Lloyd: It is exactly one of the burning questions that the steering group has been debating. By having one challenger bank in the steering group, we had that perspective at the table. In the consultation exercise we carried out, a number of banks and consumer groups, actually, raised the competition dimension that this kind of approach might have. Are we putting in place requirements that new banks will struggle to put in place? We felt overall that, although that is obviously a consideration—open banking came up earlier, and that is something that is a fact—having confident consumers, protected across the whole market, is good for competition in itself.

In terms of how quickly banks are signing up, clearly there is a lot that they need to do. Those that were closest to the development of the code are more likely to be putting in place the standards for themselves more quickly, simply by being closer to the detail. When we published the draft code in September last year, there was a commitment by the banks that were directly part of the development of the code to start putting in place those standards straight away. There was no delay because of the need to consult, but in terms of getting the whole industry on board, signed up and putting in place all the standards there is a lot further to go for some banks than for others.

Q796 **Mr Baker:** I just want to press you on that one point, because it feels like we are admitting that this is additional work and therefore it is potentially a barrier to competition and to new entrants. You implied that it is pro-competitive to protect all consumers. I am sure we do want to protect all consumers and you are nodding. Could you explain in what sense you see this new additional work as being pro-competitive? It surely must impose new costs on new entrants.



HOUSE OF COMMONS

Richard Lloyd: It imposes costs on all banks, ultimately, once they have joined the code. If you are a consumer looking at the market, and you are worried about fraud, about the impact on you, that your money may end up being taken by criminals and about what is going on in the wider ecosystem, if you do not have the sense that there are proper standards in place to detect and prevent fraud, if you do not have a sense that if you are tricked and you have done nothing wrong you will get proper help, you are probably more likely to stay with an incumbent bank than to take your business to a challenger or to a more innovative fintech firm.

It is about giving people the confidence to engage with the competitive landscape rather than to stay with the familiar, which you may, rightly or wrongly, believe to be better protecting you.

Q797 **Mr Baker:** I see. If I may put that in my own words to check I have understood, you are saying it is pro-competitive in the sense that consumers are more likely to switch, rather than in the sense of encouraging more entrants. Is that right?

Richard Lloyd: Yes, precisely so. The conditions under which anyone gets a banking licence in this country include that they will deal with crime, take steps against money laundering and so on. It is a condition of being in the marketplace and this is another aspect of that.

Q798 **Mr Baker:** At the point the code launches, what proportion of consumers would you expect to be covered? How do you expect that number to develop?

Ruth Evans: Starting with the seven I have already mentioned, that will cover about 85% of the market of consumers. That is a significant number. I do not think it will be terribly long before we get up to the 90s, depending on who signs up when. We are pretty confident that the vast majority of the market is covered.

Q799 **Mr Baker:** How will you make it clear to consumers that they are covered? You are talking about switching and so forth. If you get to the point that only 10% are not covered, how will they know?

Ruth Evans: We are doing a lot of work on this. Essentially, we are going to be producing information. The banks themselves and the providers are going to be doing their own work, but we are ensuring that there is a guide for consumers and a guide for consumer practitioners, those who are going to advise consumers. That work is under way. The reason for the gap between the publication of the code on 28 February and its enactment on 28 May is precisely in order to do this sort of work.

There are still a few governance and related issues that we are developing during that three-month period, to make sure that as many providers as possible can sign up and will sign up, and that we have the right information there at the right time for consumers, so they are fully aware of their rights.



HOUSE OF COMMONS

Q800 Mr Baker: Finally, with apologies to any colleague who is going to come back to this, what would you say to people who in the past have suffered devastating frauds of this kind? What would you say to them? Are they going to find that they will be covered as this code comes in or is it too late for them?

Ruth Evans: I am afraid it is too late for them. We are very sympathetic to them and mindful of their situations. We do not underestimate at all the devastation that, in many situations, has been wrought on lives. All we can do at this point is to say that that devastation will not occur in the future. It was made quite clear by both the PSR and UK Finance, which have worked with us on this.

Again, I would like to pay tribute to the work that both of these organisations have done in guiding and supporting the steering group, making sure that we get over the line with this. They obviously felt individually, not together, that it would be impractical and legislatively impossible to confer rights onto consumers when there was not a code already in place. From 28 May, those rights of consumers will be protected, going forward.

Q801 Chair: Following on from that, have you heard any suggestions, though, that any payment service providers might themselves decide to look at old claims in the light of the code? Do you think everyone is just drawing a line and saying, "It will be different from 28 May onwards"?

Ruth Evans: We know that, already, at least 20% of claims are met through good-will payments and it is up to the individual banks. That brings into play the competitive issue that Mr Baker was talking about. Banks will want to position themselves to view sympathetically those claims that have already been made and are not covered by the code.

Q802 Chair: Last year, £354 million was stolen as a result of authorised push payment fraud, with over 80,000 victims. As Steve has said, the consequences can be absolutely devastating. We have heard that in evidence before this Committee. Perhaps, in layman's terms, you could set out how the code is going to help victims of the future.

Ruth Evans: We are talking about individual customers here, which is £228 million, still a very significant sum, involving 78,000 consumers, with the latest figures that have been published by UK Finance. This code, in very simple terms, commits banks to do more than ever before in order to prevent fraud in the first place. That is through better detection, warnings and improving systems. Secondly, it also makes it clear to consumers what they need to do in order to protect themselves and what is required in terms of meeting their own responsibilities and obligations. Thirdly, and crucially, it takes a fresh look at the issue of vulnerability and how vulnerable consumers are covered.

The single most important principle to come out of our code is that, if consumers have done nothing wrong and have met their requisite level of



HOUSE OF COMMONS

care, as it is called, it is absolutely right that they are reimbursed. That principle has been agreed and will apply from 28 May.

Q803 **Chair:** Earlier on, you might have heard—I think you were both here—Mr Elphicke asking our previous witness about the confirmation of payee changes. You were saying there that there was going to be an obligation on the banks to keep doing more to try to stop these scams occurring. Do you or the steering group have any expectation that the confirmation of payee changes will have a positive impact on bringing down the number of scams?

Ruth Evans: Broadly speaking, yes. The steering group is waiting with some expectation for confirmation of payee to be introduced. However, just to caveat that, concerns have been expressed, within the consumer sections as well as with the banks, that, unless the right instruments are applied and we have got it right technically, there could be some detrimental impact on consumers. We want to make sure that confirmation of payee is introduced as early as possible, but that it does not have any adverse risks. Richard might want to add to that.

Richard Lloyd: The date for the introduction of confirmation of payee, as you know, has not been set yet. The PSR is still consulting. What was a very important decision by the steering group was not to wait for confirmation of payee to be available before introducing the code. It is in the code as one of the things that firms should do as one of their standards, but as a holding place pending the date being decided. Other tools may emerge and we did not want the good work of improving standards and getting consumers' clear rights to be reimbursed held up while there was uncertainty about the introduction of that particular tool.

Q804 **Chair:** Are there any types of fraud that are not covered by the code? Is there anything customers should know, if they have done all the right things and they have behaved in the right way? Is there anything people should know, or any exemptions that people should be aware of?

Ruth Evans: No, not in terms of authorised push payments. Is that right?

Richard Lloyd: That is right. It does not cover international payments, because it is a code for the UK only. For unauthorised payments there is a different regime. There have been existing legal rights for consumers. This is very explicitly defined in the code as directed at payments where the customer has authorised it or been tricked into authorising it. As you all well know, that is the growing problem that this is trying to address.

Q805 **Chair:** Catherine was giving an example earlier of money mules, what people know and what people do not. There is also going to be a practitioner guide, as I understand it. What is the timing of that? How is the drafting of that going?

Ruth Evans: It is going.



HOUSE OF COMMONS

Chair: It is happening.

Ruth Evans: It will be available by 28 May. This is one of the building blocks that we are putting in place. The practitioners' guide is being overseen by both a consumer and a PSP, with input from everybody from the steering group as well. That is a live issue at the moment, along with the consumer guides.

Q806 **Chair:** Would you have liked to have those sooner or is that, again, just an issue of lots of different views around the table?

Ruth Evans: We are pushing for everything to be sooner rather than later. The earlier that we get the information out, the greater the success rate will be from a standing start of 28 May.

Q807 **Chair:** Why does the code not have a specific section to easily set out what consumers are expected to do? Is it down to the individual banks to set what consumers are expected to do? Is that potentially going to be inconsistent where people perhaps have accounts with a number of different institutions? Is there a danger of inconsistency?

Richard Lloyd: The purpose of the practitioner guide is because the code is obviously written in a particular way. The practitioner guide gives a very clear set of examples of what kinds of activity the banks should be undertaking and what view they should take of different consumer approaches to the level of care. Some of that inevitably will come through as the code gets implemented. One of the things we have set up is an early review of how banks are interpreting what consumers did, certainly in terms of whether they checked whether the payee they were sending money to, the beneficiary, was legitimate. There are things that may need to be looked at again. It is not a code that is set in stone for all time.

The practitioner guide is intended to give people on the frontline a clear sense of what is expected of them across the industry, what good looks like and what is unacceptable. For that reason, there is a discussion going on at the moment about how widely the practitioner guide should be disseminated. We obviously do not want it to become a guide for fraudsters too. In terms of clearly articulating what the consumer should do, in a way that people can engage with and understand, the consumer groups are playing a leading role in that. The banks will do that. There is a commitment under the code to a general public awareness campaign as well.

Q808 **Chair:** Will you keep that under review in the sense of consumer groups? If it is pretty clear that consumers do not understand what their obligations are, will there be an opportunity for redrafting or further clarification?

Ruth Evans: Yes. As you will appreciate, the LSB is going to be taking over the governance of the code. The memorandum of understanding, which we are discussing tomorrow in the steering group, sets out quite



clearly the evaluation mechanisms that are going to apply as the code unfolds: thematic reviews scrutinising particular areas of the code. The practitioners' guide will be subject to review. The whole code will be reviewed. We are building evaluation of aspects of the code into the memorandum of understanding.

Richard Lloyd: Importantly on that, there will be sources of evidence about how effective the code is—we may want to come on to this later—from statistics gathered centrally, from the Financial Ombudsman Service's experience, from consumer groups, and from groups and charities that are advising consumers. Those sources of data about how effective the code is being will be built into those reviews. Consumer groups will be able to trigger reviews of particular aspects of the code, if there is evidence that that needs doing.

Q809 **Chair:** We will come back to that in a moment. Lastly, you mentioned vulnerability. You will know that we have done an inquiry, and, Mr Lloyd, you gave evidence, on vulnerable consumers' access to financial services. There is a carve-out, as you said, that anyone who could be deemed vulnerable to APP scams should be reimbursed. That is assessed on a case-by-case basis. To this point about consistency across the sector, what is the mechanism to make sure the financial institutions are applying the vulnerability test on a consistent basis?

Ruth Evans: This is a very thorny, difficult and innovative part of the code. We are at the moment working on this, because we have introduced a notion of vulnerability that is dynamic and has not been done before. We are not saying that vulnerability covers the usual suspects. A lot of people mention the mother-in-law, particularly bankers. They always talk about the mother-in-law to us. This is not about that. This is about how we are all consumers, and we all may be at any time, depending on circumstances, vulnerable. We are in the process of writing out what this vulnerability means and how it can apply consistently across the sector. It requires careful drafting and has caused a lot of scrutiny within the group, from both banks and consumers, to make sure there is a consistent definition.

Q810 **Chair:** We await that. The public awaits that draft, or that wording.

Richard Lloyd: The wording is in the code. It is very clear.

Q811 **Chair:** Sorry, I mean the underlying interpretation, but that is really for the financial institutions.

Richard Lloyd: As for how it is implemented, there is always a risk with this approach that it will be interpreted by people on the front line or by banks differently. In the future governance of the code, that is an area that I would expect early on to be audited, spotted and, if there is an inconsistency problem, addressed, either firm by firm or across the industry. The steering group was very strongly in favour of this, as Ruth says, quite innovative definition, because we could all be vulnerable to a



HOUSE OF COMMONS

scam at any time, however sophisticated or even how leading a banker we might be. There is no typology of vulnerability in this context.

Chair: Sadly, we saw the case last week of the former Deputy Governor of the Bank of England. It was very brave of him to come forward and much appreciated by consumers.

Q812 **Mr Clarke:** One of the defining features of the code is that it is voluntary. Your consultation was told last autumn by MoneySavingExpert.com that, if consumers fall victim to a scam and the at-fault firm is not a member of the code, the code becomes meaningless and the intention for consumer protection evaporates. What led to the position that the code should indeed be voluntary rather than mandatory?

Ruth Evans: That was a topical issue. It was not really one for the steering group, although we touched on it, because we of course were charged with producing a voluntary code. The reason for that is that the PSR felt this was the best way forward. The reason for that is that it could be done and introduced far more swiftly, and more responsively to consumer and industry needs, if it was done on a voluntary basis. This has caused some contention within the industry, I know, but on the whole it was not a question for the steering group, because we had a job to do.

We all recognised that a voluntary code needed to be introduced swiftly. There was consumer detriment. We needed to responsibly have an answer for that. Introducing a voluntary code in the way that we have, in essentially a year, is much faster than any statutory underpinning, which would require legislation. As you will know, at this particular parliamentary time, that would be a hard thing to achieve.

Mr Clarke: Indeed, achieving anything at all is hard.

Chair: We might all agree on it, actually.

Q813 **Mr Clarke:** How effective do you think the voluntary nature of the code will prove to be? Will there be any form of built-in review as to whether, in fact, it needs to be made mandatory at a future date?

Ruth Evans: Yes, time will tell. We believe it will be successful, because straight away we have the majority of the market covered. It depends on numbers. I expect that providers will be clamouring to join on a phased basis, as and when they are able to. As we have already explained, there is a built-in review of both the code itself and the elements of the code in the memorandum of understanding. That will be on a rolling basis. There will be a review of the code within the first year. Then there will be rolling reviews every three years.

Q814 **Mr Clarke:** That will encompass the issue of whether the voluntary nature is adequate.

Ruth Evans: Absolutely, it would cover everything.



HOUSE OF COMMONS

Richard Lloyd: There was a very interesting discussion earlier about incentives. A key principle behind the code was that we needed to find a mechanism to incentivise those best able to prevent fraud to do so. That is one measure of success of the code: has this prompted banks and others in the marketplace to do much more to switch off and attack fraud in the first place, because if they do not it will cost them? That economic incentive was central to what we have developed.

Q815 **Mr Clarke:** What happens to the customers of a PSP that is not a signatory to the code for whatever reason, because it has not yet signed up or because for some reason it has no intention of doing so?

Ruth Evans: The same as happens now. They will have to rely on the voluntary arrangements arrived at by their banks. About 20% of customers are reimbursed, as I have already indicated. I am afraid they will have to carry on relying on that. That gives them an incentive to look at whether their PSP is a member of the scheme.

Richard Lloyd: In addition to that, the PSPs that have joined the code have committed to doing their level best to extract and repatriate money from a receiving bank, if they are not a signatory to the code, to work with them and to persuade them to do the right thing. As you know, the Financial Ombudsman Service now has jurisdiction over both sending and receiving PSPs. A customer can now complain to the FOS, even if their bank is not a signatory to the code either as a sender or receiver of their money. The FOS will take into account the code in making its decisions on this.

Mr Clarke: That is really helpful. Thank you both very much.

Q816 **Chair:** That goes to the heart of public education being very important, so that consumers are aware that the bank they are with or the PSP is a signatory to the code or not. Will that information be easily available online? Will there be a comparison, rather than them having to scabble around on each bank's website looking for the information?

Ruth Evans: It needs to be easily accessible. That is what we are working on, exactly that, so we can make consumers aware.

Chair: You could have a listing.

Mr Clarke: Or a kite mark or something.

Q817 **Chair:** The trouble is that you have to scabble around on a website, looking for something at the bottom in the terms and conditions, which is not what anyone is going to do.

Ruth Evans: I suspect that banks will want it right at the top of their list of attributes.

Chair: Let us hope so.

Q818 **Rushanara Ali:** I am going to start with the code again. There is a nice, seamless transition into keeping the code relevant. Just on the steering



HOUSE OF COMMONS

group, can you say what is going to happen to the steering group?

Ruth Evans: The steering group will wind up. It is intended that the steering group winds up when the LSB takes over formally on 1 July. The code becomes live on 28 May, but the LSB takes it over on 1 July. It is possible that the steering group will be asked to reconvene to look at issues as the code develops, but it is not intended to keep it in place long term. There has been a huge amount of good will from both sides and they all want to be released at some point soon.

Q819 **Rushanara Ali:** Do you think the code will be measured and monitored appropriately?

Ruth Evans: Yes, I do. That is what we are working on with the LSB now. I am sorry to keep referring to the memorandum of understanding, but that is the working document that will show how the LSB is going to take this on and how it has the capability to take it on, including monitoring arrangements. Some of those arrangements will involve continuing to liaise with members of the steering group, a constituency of consumers and a constituency of PSPs, in name, even if not in form.

Q820 **Rushanara Ali:** Do you see the significance or relevance of this code for other areas of economic crime that consumers face? Do you think other sectors could learn, for example mobile phone companies? Have you been sharing the good practice or the thinking?

Ruth Evans: We have not, as a steering group, worked beyond our remit with the banks. However, we have had some discussions with the banks. I had a recent discussion with Barclays last week about its concerns, to see if we can use the steering group's work as an exemplar to encourage this sort of code being applied across sectors, whether it is through internet providers, social media or telecoms companies. This would make the life of banks much easier and of course, for the banks, their primary purpose is to reduce consumer detriment, as it is ours.

We hope very much that another initiative will come into play that learns from the work that we have done. It is more challenging, because it is a more disparate group, but it is essential in this era of fast-changing technology.

Richard Lloyd: Regulators outside of financial services, including the ICO and Ofcom, are discussing with the FCA and the PSR how there can be a more cross-sectoral approach to dealing with fraud. That has been a very healthy, positive outcome of this process.

Q821 **Rushanara Ali:** Yes, because the technology world does not operate in silos.

Richard Lloyd: It does not.

Q822 **Rushanara Ali:** I know you are trying to disband, but is there any mileage in some of the people in this group, perhaps you, Ms Evans, and some people who have relevant expertise, transitioning into establishing



HOUSE OF COMMONS

something that brings in additional experts to respond to the wider implications of what you have done and its benefits to others? That way, we are not losing time; we are seamlessly moving on to looking at these other sectors that could benefit from what you have done so far and build on it.

Ruth Evans: It is fair to say that we have been very pleased to do the work we have done with the steering group. As I say, the consumers have been incredibly dedicated, as have the banks. This has all been done in their own time. I am sure that many of us would be very happy to continue working, to ensure a wider application of our methodology.

Q823 Rushanara Ali: Great, thank you. Moving on to funding the reimbursement, under which circumstances will a customer be reimbursed? Who provides the funding in each scenario?

Ruth Evans: Under the code, the new approach to reimbursement, which takes effect from 28 May, means that consumers will be reimbursed if they have shown the requisite level of care: in other words, they have done nothing wrong. In the unlikely event of no blame on either side, banks have committed to funding these cases to the end of this calendar year, 2019. They are committed to finding a long-term solution for funding. At the moment, it looks most likely to be some sort of transaction levy, which could be operated through Faster Payments. Discussions are taking place between UK Finance, which is responsible for this area of work, and Pay.UK, to this effect.

There is a third tranche of customers in which there is shared blame. In the situation where there is shared blame, the funding mechanism is going to be apportioned between the banks. It is quite a complicated formula because it involves the receiving bank as well as the originating bank, and indeed the consumer. That formula is being worked out at the moment before we go live.

Q824 Rushanara Ali: How would a transaction levy work?

Ruth Evans: It would be a levy on transactions, which the banks would take the hit on. It would be up to the bank to charge or not charge its customers as it thinks fit. There is another competition issue for you.

Q825 Rushanara Ali: The banks will charge consumers to pay for their mistakes.

Ruth Evans: They could pass on the charges, or they may not pass on the charges.

Q826 Rushanara Ali: You have not given a steer. What is your judgment on what should happen? Are you staying neutral on this?

Ruth Evans: The steering group has not given a view on this.

Q827 Rushanara Ali: Why is that?



HOUSE OF COMMONS

Ruth Evans: Candidly, because to get to the point that we have got to is extremely good news. It is a significant win all round that the banks and consumers have agreed that, in the scenario of no blame, customers need to be reimbursed. That principle has been achieved.

Q828 **Rushanara Ali:** Consumers may have to pay for that in some of the banks. You are suggesting that some banks may choose not to pass on the costs through a transaction levy.

Ruth Evans: There may be a transaction levy. It depends how it works. Let us suppose there is a transaction levy across consumers, for example, and not taken by the banks, which is not the case and has not been agreed. That would be something like 1p per transaction, and there is an average of 12 a year. There is a small cost that could be applied across the piece to consumers.

There is also a feeling within the consumer groups, exactly as you say, that it is not reasonable for consumers to have to bear these costs when they have not had any fault. Some banks feel the same and some do not. That is for another day, and it is not for us as the steering group to determine. The principle of reimbursing customers who are not to blame, when the banks are not to blame, is a significant win. It is being worked out how that levy will be applied.

Richard Lloyd: I know the Committee has already heard from banks on precisely this issue. I think it was Nationwide that said, were that to be the long-term funding solution, it certainly would not pass the costs through to consumers. There may be differences of approach, but the mechanism itself is going to be worked up over the next six months.

Q829 **Rushanara Ali:** Why would they have any incentive to invest in dealing with state-of-the-art systems to prevent fraud if they could pass the costs on to the consumer?

Richard Lloyd: The code requires them to. We are talking about the no-blame scenario and the funding of that, but for the vast majority of cases at the moment, where the customer had done nothing wrong, the bank would have to reimburse the consumer. There is a cost and incentive there, but there are also, in the code, all the requirements to put in place the systems to prevent it in the first place, which would then reduce their cost.

It is important to note that the quantum, the actual size of the no-blame scenario, is hotly debated. Nobody knows, to be honest, because the code has not been implemented yet. Some view the size of the customer base that there would be in a no-blame scenario as likely to be very small. For example, there would have to be a mule account involved, so perhaps there would always be a receiving bank to blame. There is a hot debate going on about just how big the so-called no-blame problem actually is.

Q830 **Rushanara Ali:** I have two questions related to this. First, you



HOUSE OF COMMONS

mentioned that they are required to by the code but, frankly, banks do not have a record of behaving themselves over the last decade. Why should we believe that a voluntary code is going to make them do what we think is in the consumers' interests? Why do you expect us to believe that, or that the banks will behave appropriately? They did not even respect much more stringent provisions under the law.

Ruth Evans: With respect, it is not our job to believe in anything. We have been charged with producing a voluntary code that will have results. We have done it within a year, and it will provide significant benefits for consumers.

Q831 **Rushanara Ali:** I appreciate that and that is great, but my job is to interrogate the outstanding dimension to this, which is that, if the banks can pass on the costs in relation to these sorts of cases, the incentive to deal with this is, frankly, not going to be as good as it should be. We are back to that situation where banks, time and again, find ways to wriggle out of responsibilities that they should take. My worry is that they are not going to be as forthcoming in investing in what is required in order to prevent this stuff from happening in the first place.

Ruth Evans: As Richard has already said, some of the banks that we have worked with have already indicated that they will absorb the costs, and that will provide them with a market opportunity.

Q832 **Rushanara Ali:** Are the smaller ones the main ones that you think we will find are going to struggle to do that? Is that roughly how you would cut it? It would be understandable, but it is good to know.

Ruth Evans: We honestly do not know and that is why we need to review it. We have built in a review within a year. You are right to be concerned. There is good will. We do have a year's review. The other important thing to say is that you will see a cultural shift. The fact that we have this now means banks have accepted that, in the situation of no blame, consumers need to be reimbursed. That is going to osmose over the next year. It will soon be something of the past that banks think about it in the way that some of them do now.

Q833 **Rushanara Ali:** I do not want to put a downer on banks, but look at the lack of a cultural shift. Yesterday, there was a story about a former RBS executive getting another well-paid job after the global restructuring scandal, which has cost lives and damaged a lot of lives. Why should anyone believe that there is good will? There is some good will, of course. As I keep saying, some of my good friends are bankers. That is not the point. The point is that, as a system, there are massive problems and they just carry on, and consumers do not get the fairness they deserve.

Ruth Evans: You are echoing many of the arguments put in the steering group and I have huge sympathy for those. They have been articulated. Of course, we are not unaware of the behaviours of the banks over the years. That is why we were asked to do this work. We are not naïve, but we have achieved a significant gain. All I can say is that we will be



HOUSE OF COMMONS

watching this closely. Richard might want to give you further reassurance.

Rushanara Ali: Richard, go ahead.

Richard Lloyd: I will do my best. You are quite right: the Committee needs to be questioning and sceptical, as indeed were many of the consumer groups and the banks themselves about the nature of a voluntary code and its effectiveness. If banks choose to hide behind the no-blame scenario and impose costs on consumers as a result of that, it will become evident very quickly. Across the industry, some have said publicly that that is not what they are going to do. If others choose to go down that road, they will risk losing even more trust and credibility, and potentially customers. They will need to come and account for themselves to you.

Rushanara Ali: Some of them do not seem to mind that. We are still waiting for another bank to give us the findings of an inquiry that has been commissioned, to tell us why tens of thousands, nearly 100,000 people, had huge disruption because of a technology failure. Those things are increasing. Your other review of the FOS did not go, in my view, far enough. While you are here, I might as well have a go at you about that. It did not seem to go far enough to stand up for consumers. You did not allow for the tribunals. There are major questions about costs.

Chair: We are not talking about that today. We are talking about the code.

Q834 **Rushanara Ali:** The point is this. It is actually quite unhelpful to have to think about this stuff in silos, because the banking and consumer world does not operate like that. Our lives are not in silos. These different things are happening. You have given your time; you are providing a public service, so I do not want to be too down on that. It is not that, but the lack of cohesive thinking means that we keep having to come back to things a year or two years later with different Committee members and so on. It is not always easy to hold institutions to account when you have so much flux going on, both systemically in the sector and here in this place.

Richard Lloyd: Can I just say something about the FOS? We have discussed this before, I know. The code gives consumers another clear framework to take a complaint to the FOS. There are provisions for that in here. The FOS has been given more powers, whatever you think of their effectiveness. In the case of individuals who previously have been turned down for reimbursement, there is now a very clear reversal of the principle, which is that you will get reimbursed unless you have done something wrong. The FOS will take its own view of that, but it will take the code into account.

Over the next year or so, we will need to make sure that consumers are very aware of what they need to do to take care, but if they get a decision they disagree with, if they are blamed or the bank says, "We did



everything we could; we are blameless as well”, they have the absolute right to go to the FOS, complain and get their money back through that route. I know there are not straightforward, simple, system-wide answers here, but it is about giving the consumer more tools.

Q835 Rushanara Ali: Do you think the FOS has the resources to deal with yet another set of responsibilities that we are asking it to take on?

Richard Lloyd: On this, we have been working with them over the last year to make sure that they are very clear about what is coming and are tooled up to deal with this. In fact, they welcomed it as another means by which they can be much less on the back foot about how they deal with this kind of fraud. It will help them.

Ruth Evans: Can I just be clear? This is not a standstill code. This is the first step. Actually, it is a significant first step. It is up to the Treasury Select Committee, as well as consumers, as well as the banks themselves, holding themselves to account, to make sure that it works. There was no other solution. If we had waited for a statutory code, we would not have had one for another two or three years. We now have a code in place that is going to reimburse consumers, so it is a good starting point, but it is not the endpoint. You are absolutely right to be sceptical and keep everyone on their toes.

Q836 Rushanara Ali: I am not sceptical about your contributions.

Ruth Evans: I understand exactly what you are saying.

Rushanara Ali: Please do not get me wrong. We really appreciate what you have done.

Ruth Evans: I understand, but there is a well-informed and well-intentioned view within the industry that this is the right thing to do. That is what was remarkable about the steering group. It brought together very polarised interests to accept a consensus argument that it is not right for consumers to have to suffer this detriment.

Rushanara Ali: Perhaps we should deploy you on negotiating between parliamentarians over Brexit and getting a consensus here.

Ruth Evans: We do sometimes feel it is like that.

Chair: Thank you both very much indeed. As you say, we accept the challenge. We will look at the code, how it develops and how it is used, and ask those who have signed up to it how they are responding to it when they are before us, giving evidence. For now, thank you both very much for being here today.