HOUSE OF COMMONS

Treasury Committee

Oral evidence: Economic Crime, HC 940

Wednesday 13 February 2019

Ordered by the House of Commons to be published on 13 February 2019.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Steve Baker; Charlie Elphicke; Catherine McKinnell; Wes Streeting.

Questions 623 - 721

Witnesses

I: Stephen Jones, Chief Executive, UK Finance; Susan Allen, Head of Retail and Business Banking, Santander UK; Chris Rhodes, Chief Product and Propositions Officer, Nationwide Building Society.

Written evidence from witnesses:

– UK Finance, Santander UK

Examination of witnesses

Witnesses: Stephen Jones, Susan Allen and Chris Rhodes.

Q623 **Chair:** Good morning. Thank you to our three witnesses for being here. I am sorry that we are slightly in the dark over here, but you will be able to see us. We are also slightly light on the ground, due to ill health and other matters going on, but we are very grateful to the three of you for being here for the latest session in our inquiry on economic crime. We have had lots of excellent evidence from a whole variety of witnesses on this important topic. I am going to ask you all to introduce yourselves, and then we will start with some questions.

Susan Allen: Good morning. My name is Susan Allen. I have recently taken responsibility for retail and business banking at Santander. I am really glad to be here today to contribute to this discussion, which, as you know, is really important given the impact on consumers. Thank you for the opportunity.

Stephen Jones: I am Stephen Jones. I am the chief executive of UK Finance, the trade association that represents the banking and finance industry in the UK.

Chris Rhodes: I am Chris Rhodes. I lead the product and propositions teams at Nationwide, so I am responsible for all the products we offer to our 15 million members.

Q624 **Chair:** Lovely, thank you. Let us start with the overall issue of consumer-targeted economic crime. Ms Allen, as you say, this is an important issue. Sadly, UK Finance figures show that just over £500 million was stolen by criminals through authorised and unauthorised fraud in the first six months of 2018. Having said that, in the same period the finance industry prevented just over £700 million of unauthorised fraud as well. Perhaps we could start with Santander and you could tell us how high a priority combating economic crime is for your institution.

Susan Allen: This is really a top-priority risk for us. It is actually what we would consider a board-level risk. Our board pays significant attention to this issue and has regular reports on the matter. A number of the senior team are very closely involved, literally on a day-to-day basis. I personally oversee many of the situations that are more difficult for our customers. We invest heavily, first of all, in the prevention of economic crime. That is really important. For instance, in our team we have over 700 people focusing on fraud and over 600 people focusing on financial crime. We invested over £100 million last year in improving our systems to help to prevent and detect unusual transactions and to make sure that we do not facilitate those transactions.

Q625 **Chair:** Mr Rhodes, how about Nationwide?

Chris Rhodes: It is very much the same. It is a very high priority. Clearly, when customers are scammed and not refunded, it is very

difficult for them. We have a number of focuses, including the opening of accounts and making sure we are opening new bank accounts for legitimate people; the profiling of transactions that are made; and customer education, because increasingly, as security technology has improved, fraudsters are going after our members as the place where they can scam money.

Q626 **Chair:** Presumably, there are lots of initiatives that have been put in place already, but there are always more. Exactly as you say, criminals and fraudsters are constantly updating their techniques in order to try to stay ahead. One of the things that has been suggested was about when a customer puts in a payee name. It is not checked to ensure it matches with the name on the receiving account. That seems like quite a quick win. Why is that not being pursued? Mr Jones, you represent the industry more broadly. Is that something that you as a trade body would like to see being brought in?

Stephen Jones: I believe you are talking about the confirmation of payee, which is the system whereby you put in the sort code and the account number of the destination account you wish your money to go to, and there is an automatic cross-check, which will pop up with the name of the account so you can visualise whether this is the person or the entity you want to pay.

We are working on delivering that. It is quite a complex IT and process change. We are working hand in glove with the Payment Systems Regulator, who you saw yesterday, on a timetable to ensure that is put in place across the industry. I expect that will be capable of being rolled out across the vast majority of payment services providers sometime next year. It is a big change, and it is a big change at a time of a lot of changes across a number of other initiatives that the banks are being required to implement. It is not being de-prioritised. It is a very high priority as part of the overall suite of measures that is being taken and constantly updated in order to reduce the size of the fraud problem, because it is a big problem.

Q627 **Chair:** It is a big change in terms of IT? For a bank like Santander, how big a change will it be to bring this new system in?

Susan Allen: It sounds very simple but, when you think about it, our customers make payments in lots of different ways. They make payments through branches, through the telephone centres and through online or mobile banking. So when we are making these changes, we have to make changes in every single one of those channels; we have to make changes that link into the payment systems; and then we have to make changes to be able to receive messages in from the other banks and present them back to the customer in whatever channel the customer chooses.

That is quite a complex change. As Stephen says, it is at the same time as changes for PSD2, Open Banking and changes in terms of the CMA

remedies and the high-cost credit review. All of those changes touch the payments system, so we have to look at sequencing them very carefully so that, at the same time, we do not create an operational risk to the payments system. We have a pool of people in the UK, a finite pool of people, who really understand and can work on these systems. We have to sequence those changes.

I would say that we are all agreed that confirmation of payee is a really important change. Just yesterday I saw a situation where thankfully we managed to stop a scam for one of our customers when we encouraged them to phone to check the account details that money was going to. It turned out that somebody had intervened. It was one of those email interceptions, and they almost sent the money to a fraudulent account. It is really important to get confirmation of payee. We think it will make a big difference, but it is a bit more complex than it sounds at the outset.

Stephen Jones: Can I just make a competition point, Chair? There is also the issue that we want a broad variety of payment service providers in the system of all shapes and sizes. While the large and sophisticated institutions on my left and right have the resource to do what is required internally, a number of the middle and smaller-sized institutions do rely on third parties to deliver a solution to implement. What we are trying to do is encourage those third parties to come forward and deliver competitive solutions that can then be implemented by smaller PSPs. That is another factor we have to take into account in recommending a timetable for the whole system.

If we go too fast, we will end up with a two-tier system where only the big institutions are able to offer confirmation of payee, and then customers are forced to make a choice between the big institutions and mid-sized and smaller-sized institutions, who we want to encourage for competitive reasons but who do not have the resource to do it as fast as the big institutions. So there is quite a tension there in terms of execution.

Q628 **Chair:** Would you agree with all of that from Nationwide's point of view?

Chris Rhodes: Yes, absolutely. The only other thing to say is that because it requires me to send a message to Santander and for them to confirm that it is the right account, it has to work both ways. There has to be a critical mass of institutions able to test and then implement at the same time.

Q629 **Chair:** Ms Allen, you talked about a particular incident. I visited Santander in Loughborough and Action Fraud, the branch there. A lot of catching these scams comes down to individual bank staff spotting unusual patterns or people perhaps repeatedly seeing what seem like small transactions but that add up to very large or often life-changing amounts of money disappearing from their accounts. Perhaps you and Chris, on behalf of Nationwide, could talk us through staff training and how this works not just face to face in branches but also on the telephone

and particularly online as well.

Susan Allen: There are probably a number of different aspects of this that I would like to bring out. The first is that, while that final step of the payment actually being made is important, we also invest very heavily in prevention. As Chris said, one of the key things for all of the banks is making sure that when we are opening accounts we are doing that for legitimate people. We take enormous care to try to make sure we are only opening legitimate accounts in the first place, because that is the entry point into the banking system.

Beyond that, we will also invest heavily in detection, which is about looking for unusual patterns or unusual transactions. For instance, we screen payments on the way in. If a credit coming in to an account looks like it is very large relative to the account—for example, a student account—then we will block that payment until we speak to the account holder and make sure that is a legitimate payment into the account. We block credits on the way in if they look like they are going to an account that looks out of line. There is huge investment in prevention, first of all, and detection. That is where the vast majority of our effort goes.

It is then really important to make sure we are supporting our customers at the point they want to make a payment. We have done a number of things. First of all, in our digital channels, when people are keying payments online, last year we introduced a series of warnings. Depending on what you say the payment is for, a message will drop down or pop up on your screen that will give you some hints and tips to be aware of. We are particularly looking out for high-value payments like people paying solicitors, where we know we have had examples of emails being intercepted. We will give people tips to say, "Actually, just take care. Have you independently checked that the payment is going to the right account?" If you are buying goods, we will give a particular hint about that. This is in the payments process in order to try to give that moment for customers to reflect. Often in these scams people are being pressurised to make decisions very quickly. Particularly when it is a digital payment, there may not be anybody around. So it is really important to give information to consumers to help them to take a moment. Stephen might want to pick up on Take Five, but that sort of idea of taking five is important.

In our branches and contact centres, we have another opportunity to have a conversation with the customer. That is really important. We do provide training to all of our staff in contact centres and branches—that is about 12,000 colleagues—to make sure we are asking questions. We continually refine the guidance we give. A few years ago, we used to read quite a standard script to customers, but we realised that people were almost tuning it out because it sounded like corporate speak. We have worked really hard with consumer groups and with our own staff to test different wordings and to make it much more natural.

Nonetheless, I should say that there are still examples of this. I have seen one case where we read the script to a customer 20 times on different occasions and in different locations, and they insisted they wanted the payments to go ahead, and those payments were to fraudsters. There is no silver bullet here; it is very important to try a range of things. That training is provided to frontline staff in branches and contact centres. In addition, we do a lot of work to help, we hope, to educate our customers on how to keep themselves safe. Last year, we ran a particularly successful initiative called Scam Avoidance School. We took that around the UK, not just in our branches. We worked with Age UK and Barnardo's; we ran it in community centres. This programme provided people, not just our customers, with hints and tips on how to stay safe online. About 20,000 people attended those. There is a whole range of different interventions we would undertake.

Q630 **Chair:** At Nationwide, what is your experience in terms of staff training and the different methods for people getting hold of their money?

Chris Rhodes: Again, it is very similar. Branch and contact centres now have a standard form of questions that they work through to understand what the payment is about, where it is going and whether the customer knows who the payee is. All that gets checked as a payment is initiated either in the contact centre or the branch. The advantage that branches have is that quite often they know the customer and therefore that this is an unusual transaction for them. Similar to Santander, you can challenge customers and ultimately sometimes they insist a payment needs to be made. Those are some of the most difficult cases.

When we think about the electronic world, we will be bringing our experience of the questions we have used in the branch network into our online journeys at the beginning of March. What we have seen in the network is broadly a 20% fall in scams by the use of those challenge and education questions.

Q631 **Chair:** This is in the branches.

Chris Rhodes: Yes, that is in the branches.

Chair: You are now going to bring it online.

Chris Rhodes: We are going to bring it into the online journeys to challenge you: "What is the payment about? Do you know where it is going? Have you checked who you are paying? Is that the right account number?" It is about asking all of those kinds of questions to make sure you have done your due diligence about where a payment is going.

We also, as the whole industry does, do scanning of payments. Within the Faster Payments scheme, you are allowed to delay a payment for up to two hours. We suspend and delay up to 1,000 payments a week to do further investigation before they leave the society. About one in 20 of those turn out to be fraud. We then have account profiling in terms of any payments that are being made out from an account. Are they

unusual in nature? Is it a typical transaction that you would expect a customer with that profile to make?

Q632 **Chair:** Before I hand over to Charlie, it is quite a job to stop payments, speak to customers, ask them whether this is where they mean to send the money and do everything else. I am not sure whether you will be able to say this, but roughly what proportion of your staff carries out this work?

Chris Rhodes: In terms of the branch network, that is training for all of our frontline staff, what we call customer representatives. That is in the order of 3,000 or so people, who have to be trained in how to spot these things on the frontline. There are 300 or 400 in the contact centres, and then we have 24-hour fraud operations scanning for payments going through the systems.

Q633 **Charlie Elphicke:** Stephen, can I start with you? Can I ask you for your views on the role of the Financial Ombudsman Service and whether it should be compulsory?

Stephen Jones: You mean compulsory as the arbiter of a dispute about whether a fraud has been committed? Are we talking about fraud reimbursement here?

Charlie Elphicke: Yes.

Stephen Jones: The first line of decisioning, in my view, should always be between the paying and the receiving bank when a customer has fallen victim to a fraud. There is a protocol that exists and, as you know, we are developing a code that will make it much more consistent across the payments system. As the second line, in the event the victim is not satisfied with the resolution regarding whether or not reimbursement should have taken place, the ombudsman is the appropriate place to go. That is the second line, as opposed to the first line, of resolution.

In most cases where a fraud has been committed and the customer is either innocent or a vulnerable victim, the banks will repay and there is no need for the ombudsman to get involved. The ombudsman only really needs to get involved where there is a dispute about liability for the fraud that has been perpetrated on the customer.

Q634 **Charlie Elphicke:** Should it be compulsory as a form of second line?

Stephen Jones: You mean as the referral mechanism. Under the APP CRM code, we are proposing that the ombudsman be the second line. Every signatory to that code will automatically refer, to the extent that there is an issue of liability, whether the customer has acted with an appropriate degree of care or not. If the customer believes they have and the banks believe they have not, that will get referred to the FOS. That is the intention under the code.

Q635 **Charlie Elphicke:** My concern is it seems a little bit hazy as to whether it

is voluntary or compulsory. Some banks might feel they can choose whether they want to participate or not. I do not know about you, but I do not think that is really good enough.

Stephen Jones: There are many aspects of the APP CRM code that would frankly be better done by regulation, but the regulator has declined to regulate.

Charlie Elphicke: This is the Payment Systems Regulator.

Stephen Jones: Yes.

Q636 **Charlie Elphicke:** So we need some improvement at the Payment Systems Regulator. We need them to be very clear on regulation and to say, "This should be the second line".

Stephen Jones: If liability were introduced by way of regulation as opposed to a voluntary code, there would be less room for doubt and error. There would be less wiggle room. I have to say, however, these two institutions on my left and right and the other four members of the steering group are working extremely hard to build a robust code, which will be followed in a consistent manner and offer victims an absolutely crystal-clear experience and a much better resolution when they have fallen victim. If a victim has done what they are required to do under the code, which is a pretty low bar, in terms of protecting themselves, then under the code the banks will repay if they are victims of fraud. We hope that consistent and clear experience will be signed up to by the vast majority of payment services providers across the United Kingdom.

It is going to take a little bit of time to implement through this year and to get everybody other than the founding six signed up, but I am pretty confident that all of the hard work that has gone in, including with the Payment Systems Regulator and the third sector, to execute this code will deliver a much better and more consistent experience for victims, with much less room for dispute in terms of whether someone should or should not be reimbursed.

Q637 **Charlie Elphicke:** Susan, an appeal mechanism is not a bad idea, is it? It would give some consistency so a bank that might say to their customer, "We do not want to reimburse you", then knows they have to answer against a set of principles that will be imposed by the Financial Ombudsman Service. Let us take a case that involves Santander. You talk a good game today, but you fought a customer of yours who you refused to reimburse £12,000 until you were ordered to by the Financial Ombudsman Service. Does that not show that it is effective and important to have that kind of consistency?

Susan Allen: It is really important to have consistency. First of all, we do care very deeply about the cases we see that come across the desk. Certainly, I see some cases that are really difficult, which really have been life-changing for our customers. We take those extremely seriously. As Stephen said, in all cases where the bank is at fault, the bank will

reimburse the customer as quickly as possible. That is not in question. There are some cases where we have a slightly more subjective decision to make as to whether we think the consumer, the customer, has done everything they could to protect themselves and whether the bank has done everything it could. Where the bank is at fault, we will absolutely reimburse.

The definition of what is expected of customers is moving over time, as fraudsters become more sophisticated. It is fair to say that we and FOS have moved over time in terms of our view as to what is acceptable for customers to do and what would be unreasonable to expect customers to do to protect themselves. That definition has moved and is moving. That is right, because the nature of scams is changing. There will be occasions when we will take a view and the case will go to FOS. We will have a discussion with them and we will take their views.

It is right that we do, on occasion, reflect and say, "Actually, we think that is right". I do not know the details of the specific case you mention, Mr Elphicke, but I assume that is what happened in that case. The other thing I would just say is that where that—

Q638 **Charlie Elphicke:** Let me just stop you there. In this particular case, it seems to me that you must be moving awfully quickly. This case was published on 11 January 2019. Caroline Wayman, chief executive of the FOS, said that it was not fair to automatically call a customer grossly negligent simply because they have fallen for a scam. It looks like Santander had some kind of policy of just telling any customer, "It is all your fault. Go away". Have you changed your practices?

Susan Allen: That is absolutely not the case.

Q639 **Charlie Elphicke:** Have you learned from this case?

Susan Allen: Absolutely, yes.

Q640 **Charlie Elphicke:** What are the learnings you have had from this case?

Susan Allen: There have been a number of cases that the FOS has been reviewing over a period of time. They had a stock of cases from over six months that they were working through. We started to have their views on those cases earlier this year and we have been working with them. We have another 124 of them that we are working through with them and we will have completed in the next couple of months. On some of those, their views have helped shape our decisions.

For instance, in one case that I am very well aware of, we made a decision to reimburse the customer. Not only did we reimburse that customer but we have gone through the rest of the 124 to look for cases with a similar pattern and we have reimbursed those customers. We have gone back through the cases we have seen over the last few years that have had a very similar modus operandi, and we are in the process of writing out to those customers to reimburse them as well. It is a

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

Q641 **Charlie Elphicke:** Have you changed your policy so you do not automatically call a customer grossly negligent?

Susan Allen: We have never automatically called a customer grossly negligent.

Q642 **Charlie Elphicke:** Caroline Wayman is saying that in this landmark decision.

Susan Allen: As part of explaining to customers why we think it is not right to reimburse them, that is language that is used. That is the language the FOS have picked up on, but we review every single case on a case-by-case basis. Even if a customer has not adhered to some of our set of principles, we will take into account, for instance, vulnerability. So there may be cases where customers have given away their PINs or their passwords or they have ignored repeated warnings, and yet we will still reimburse if we consider that the vulnerability overrides their responsibility. It is absolutely not a blanket judgment, I assure you.

Chair: Did you want to ask about the delayed payments?

Q643 **Charlie Elphicke:** I was just going to move on. The issue that also concerns me is effectively a cooling-off period. There has been a discussion about a delay of 24 hours to slow it down and give the customer a chance to think about it. Are you guys going to do that?

Susan Allen: We have actually introduced it. Customers already have the choice to change the timings of their payments. We have already done that. The only thing I would say is that on its own that is not really sufficient, because the fraudsters are quite sophisticated and they can convince the customer that they actually should not tick that box. We need more than that.

Certainly we and the other payment service providers would be quite keen to explore how we could introduce more delay into the system or more grit into the system. Everybody has got used to the convenience of faster payments and payments going very quickly. Stephen, you say that it is 0.17 seconds. I question how many payments need to go that quickly, particularly large payments. At Santander, we process 3 million payments and 5 million card payments every day. We invest heavily in detection systems to look for unusual transactions, but under the regulations today we cannot hold up those faster payments. We would certainly welcome the intervention to allow us to introduce more delays, where we believe it is reasonable.

Q644 **Charlie Elphicke:** Again, that is the regulator, is it?

Stephen Jones: It is actually the Payment Services Regulations 2017, which unfortunately derive from Brussels. It is not even just in the remit of the PSR here.

Q645 **Charlie Elphicke:** After 29 March, we can fix this quickly, then.

Stephen Jones: Maybe.

Chair: Let us not touch on that. We were doing so well.

Q646 **Charlie Elphicke:** Delay has been considered as one option. What additional ideas have the industry come up with, Stephen, to stop these sorts of frauds happening?

Stephen Jones: Confirmation of payee remains the most important new initiative, which we are all working on to try to reduce the overall size of the pot, which is, as you say, digital. There are also enormous opportunities in the FinTech world around education of the vulnerable in particular, which are targeted on particular forms of vulnerability and which enable safer usage, if you like, of the digital payments system by those who display particular characteristics of illness or vulnerability. We are seeing individual examples being developed along that line.

I would echo Susan's point that it is a very fast-moving world. Unfortunately, the victims of social engineering would not typically be who you and I might characterise as vulnerable, such as the elderly. They are typically people who are under 30 who are very overly trusting of Facebook and Instagram, for example, which are increasingly being used by organised criminals as a means of compromising payments made by people that we would assume are digitally savvy. This is a very big problem, and we all need to work fast together and not fall into stereotypical assumptions about who a victim is likely to be in the system, because, as you know, younger people tend to be more trusting of digital media.

Q647 **Rushanara Ali:** The focus of my questions is mainly on the contingent reimbursement model. Obviously, you have touched on some of this. Mr Jones, can you set out what that involves? What are your views on it being applied retrospectively?

Stephen Jones: The detail of the code is still being finalised and agreed by the steering group, which as you know is led by an independent chair, Ruth Evans, with representatives of the banks and the third sector. The most important thing about the code and the purpose of the code is for the industry to come together with the third sector and try to reduce the overall size of the authorised push payment fraud problem, which, as you know, in the first half of 2018 resulted in about £145 million-worth of victims of crime. Let us not lose sight of the fact that this is criminals who are taking money away from victims using the payments system via payment systems providers to do so. What we are all seeking to do is to reduce criminality in the system.

The next important feature of the code is the fact that there will be clearly defined standards of care, which both the paying and receiving bank have to demonstrate they have adhered to, and the consumer will have to demonstrate that they have adhered to, under the code. In circumstances where the consumer has done whatever they are required to do under the code and has fallen victim, they will automatically be reimbursed, even in circumstances where the paying and receiving banks have also done everything that is required of them. That is a very important principle.

Q648 **Rushanara Ali:** This is the "no blame" principle, where they would be covered in that situation if that is established according to the criteria.

Stephen Jones: We have reached the position now where it has accepted that we need to be able to make the statement to victims, "If you have done what is required of you in the payments system and you fall victim to authorised push payment fraud, you will be reimbursed".

Q649 **Rushanara Ali:** You are currently devising that. Lots of our constituents, and in fact ourselves, would be interested to know what those points are that we need to be mindful of. Can that be released as soon as possible so people can get on with it?

Stephen Jones: I totally agree. The chair of the steering group has asked me not to front-run with the Committee a code that has not yet been fully agreed. The committee is preparing to make an announcement by the end of this month, which will set out the future timelines for final publication of the code, with a delay then to sign up as many PSPs as possible and to undertake the education that you point to for consumers before the code is then actually implemented. Then that principle of no blame will come in. If a customer has done what they are required to do, they will be reimbursed.

Q650 **Rushanara Ali:** By the end of the month, could we expect to see some draft guidelines or not?

Stephen Jones: You will not see the full code, but you will see the principles that underpin the code. There are still a few complicated execution areas.

Q651 **Rushanara Ali:** There will, however, be enough there for our constituents to be able to look at what they need to do and revise any actions they are taking?

Stephen Jones: That is fair. You will not find that the standards are too onerous. At the moment, under the payment systems regulations, customers are required to keep their credentials safe and not to hand them over to third parties. Indeed, our Take Five campaign, which was referenced by Susan earlier, is already out there and being used across all payment mechanisms, even in the telecoms sector now.

Q652 **Rushanara Ali:** What about retrospective application?

Stephen Jones: I do not think we can retrospectively apply. With all of these changes, fraud practice is changing; standards are changing. I would try to answer that question like this. Actually, the code will change going forward as new tools come in to help prevent fraud and new ways of social engineering to create the fraud are uncovered. We will need to adapt the code in a very active way going forward. For that reason, it is quite encouraging that there will be a third-party owner of the code. We hope that will be the Lending Standards Board. As custodian of the code, the Lending Standards Board will work with the steering group to ensure the code stays alive and moves forward as the expectations of society move forward and as the types of fraud move forward.

Q653 **Rushanara Ali:** Will they be monitoring the impact of the code as well?

Stephen Jones: Yes.

Q654 **Rushanara Ali:** Just to press you a bit on it being retrospective, in the code that is being developed at the moment they are not looking at it being retrospective at all.

Stephen Jones: No.

Q655 **Rushanara Ali:** Do you know how many "no blame" cases there are over the last two or three years?

Stephen Jones: If we look at the 2018 data, assuming that 2019 is the same, we think the banks will probably be reimbursing somewhere between £30 million and £40 million more out of the authorised push payment victim pool as a result of the code in "no blame" scenarios. That is not a perfectly scientific number, but it is roughly the amount we think the banks would need to fund for 2019 if the code were up and running for 2019, for the full calendar year. We are also working on a longer-term funding mechanism, which is not just funded by the banks, but that has not been finalised yet.

It is important that we recognise that often the genesis of these frauds happens as a result of, for example, data breaches in other sectors. I do not think anyone, not even some of the consumer groups, would agree that it is fair for the banks to be funding breaches in the travel, airline or retail sectors, which result in fraud through the banking system. The Payment Systems Regulator has also indicated that it does not feel it is appropriate for a wholesale shifting of liability on to the banking system.

Q656 **Rushanara Ali:** You have mentioned 2018. What about previous years? Do you have the figures?

Stephen Jones: I do not have the data in front of me. I would be very happy to write back to the Committee with some estimates of what we think that might be.

Rushanara Ali: That would be really helpful.

Stephen Jones: As you know, we did see quite a big uplift in 2018 on prior years in terms of the overall size of the pot, so my recollection is that the first half of 2018 was 44% up on the first half of 2017.

Q657 **Rushanara Ali:** Are these "no blame" cases?

Stephen Jones: This is the total APP pot, and "no blame" cases tend to be a pretty consistent portion of that pot, but we will come back to you with the data we actually have.

Rushanara Ali: Yes, and please include "no blame" cases.

Stephen Jones: The other thing I would stress is that in 2018 more banks were submitting their data to the central pool than in prior years, so the quality of like-for-like data is not good. There were four new and relatively large institutions that were contributing to the 2018 data who were not contributing to the 2017 data. I will have to give you lots of caveats on the data, I am afraid.

Q658 **Rushanara Ali:** I just have one more question for you, Mr Jones. You said that historic cases are not being considered. Do you not think they should be? If there is no blame, shouldn't somebody pay?

Stephen Jones: It is very hard to go back. Typically, if the Chancellor changes tax laws, we do not expect him to change them retrospectively. People work within the environment they—

Chair: Let us not get into that. There is another whole area of retrospectivity that we have been talking about.

Stephen Jones: Yes, which we do not like, do we?

Rushanara Ali: This is not helping consumers.

Stephen Jones: I understand that, but it would be very hard. The third sector has accepted that it would be very hard and very unpredictable to apply a code that is engineered and designed in the context of the current incidence of fraud, how it happens and what is reasonable to expect of consumers today, compared with situations in the past that frankly are not parallel. For that reason, the most important thing is that we make the system safer, more predictable and more consistent for consumers from today, accepting that there may have been situations in the past where the journeys that consumers had were not consistent in that way.

Q659 **Rushanara Ali:** Some of those issues are system failure. I am sorry. This is my last supplementary question for you. I will ask others to contribute. Would you accept that this is a systems failure rather than an individual failure? Particularly focusing on the "no blame" cases, people who are in that category, in the past they have been failed by the system, just as, for instance, some of the mortgage prisoners were failed by the system because rules were being applied to them that were different from the ones that they were fulfilling pre-financial crisis. That is

an example of a parallel where people end up being caught in the system because institutions make judgment calls and offer services that turn out to be problematic, albeit not entirely but in part. It is just not satisfactory to have no redress for them when that is the case.

Stephen Jones: In the circumstances we are talking about where the customer is not to blame, if the banks were to blame in those circumstances in historic cases, the customer could have gone to FOS and would have been refunded. So what we are talking about is "no blame, no blame".

Q660 **Rushanara Ali:** My point is not necessarily that the banks per se should pay, but who should pay? Somebody should pay. That is the point I am trying to get to. Would you not agree? It might not be the banks, but the point is that there is an issue here, as with a number of others, where consumers end up losing out even if they are not to blame. In this case, the inference is that banks were not to blame either, given the "no blame" situation, so they are not liable. My point is a point of principle. Should somebody not be paying consumers, particularly those whose lives have been ruined in very serious cases, with larger amounts of money going amiss?

Stephen Jones: I would like to see us move eventually, on a longer-term policy basis, to an insurance-based system. That is much fairer, and it deals precisely with the situation you are describing now. When we talk about the long-term funding of APP CRM, I would expect us to move to some form of transparent insurance-based funding of the pot. It could move beyond fraud to other areas, for example, of economic crime, where there are victims and where the victims deserve reimbursement but there is no clear way to attribute liability to an individual, a firm or a specific data breach, et cetera.

Q661 **Rushanara Ali:** Ms Allen or Mr Rhodes, do you want to reflect on some of those questions? In particular, what is your view on this idea of a longer-term insurance-based model? Who would pay for it? Would consumers have to pay for it, or would there be some other way of providing that insurance scheme?

Susan Allen: The principle is a sound one. We have not yet worked through the detail of what that could or should look like or who should contribute to that. My own view is that there is a whole ecosystem of players here, not just banks, and we should look to extend the scope to all of those parties. Stephen mentioned areas such as data breaches. You can track and see correlation between fraud attempts on customers and data breaches in other organisations. That point is for all of us in terms of how important data security is. I do support the principle. We have quite a lot of work to do. Obviously, our focus right now is on the immediacy of the contingent reimbursement model and the code, but beyond that there is a debate to have about how we protect the ecosystem, what the mechanism is for that and who the participants in that need to be.

Chris Rhodes: I would agree with that. We want a long-term insurance scheme that ensures "no blame" cases can be paid on a consistent basis to customers. The system should pay for that.

Q662 **Rushanara Ali:** Is the system the institutions?

Chris Rhodes: It is the institutions that participate in the payment system.

Q663 **Rushanara Ali:** Are you sharing data? Are you co-operating with other institutions on data-sharing and how to tackle fraud together?

Chris Rhodes: Yes, there is a huge amount of data-sharing. There are even pilots taking place at the moment where we can chase payments through the system to see where they ultimately end up. It is quite difficult to get that cash back. Quite often, that cash disappears abroad. There are new technologies where we can share data and increasingly track payments.

Susan Allen: Can I just say that there is room for us to do more on data-sharing? Anything that helps us in terms of regulation to enable more of that would be really helpful. Even today, as Chris mentions, we are part of the Mule Insights Tactical Solution; we are tracking where payments go. Even when we find that money has gone to an account, today you cannot get it back. Unless you have the authority of the account holder to remove that money, you cannot remove that money even if you have suspicion. Actually, there is something that could be done in regulation to help us.

Stephen Jones: We do need legal help in that. Fundamentally, when we are talking about victims, if we can identify where the victim's money has gone but cannot do anything about repatriating the money from the end account to the victim, something is wrong in the system. Unfortunately it is the law that prevents that at the moment.

Rushanara Ali: We are going to come back to that.

Chair: We will come back to that.

Q664 **Catherine McKinnell:** I just wanted to focus on gross negligence and the working definition that particularly Santander and Nationwide currently apply to determine whether a customer's financial loss was their own fault. I know this has been referred to already, but could you just talk us through how you apply that? I am happy for you to go first, Chris, if you want to.

Chris Rhodes: Gross negligence as a concept is not actually embedded into the regulation. Clearly, FOS uses an evolving definition of it when they look at ultimately resolving complaints.

Q665 **Catherine McKinnell:** You say "embedded"; what do you mean?

Chris Rhodes: The regulations simply talk about customers looking after their security details and informing their bank if their card is lost. There is

no concept of gross negligence within the payment services directive, which is the regulation under which we run payments. The regulations per se are not the important thing. It is about how we would implement and introduce controls to protect, in our case, Nationwide members. Maybe I will give you a couple of examples of where we think the customer would be refunded and where the customer would be liable, because they have done something they should not. In order to start a payment in Nationwide, you need to use your debit card and a thing called a card reader. You put the card in the card reader and you create some one-off PINs. One scam, effectively, is phoning up the customer and telling them to put the card in the card reader and give you a series of codes. If that were to happen to a Nationwide member, we always refund in those cases.

Q666 **Catherine McKinnell:** I am sorry. Can I just stop you there? To go back to the first comment you made about gross negligence not being embedded in the regulations, it is referred to in the regulations and it is one of the criteria under which the bank would not be liable to pay the customer. I do not really understand. I appreciate that it is not well defined, but it is in the regulations. Rather than going through all the circumstances in which you would pay out, it would be helpful to understand where you understand the criteria to say that you will not pay the customer.

Chris Rhodes: I do not think it is in the regulations. Maybe we can write to the Committee.

Q667 **Chair:** It is. It is regulation 77(3)(b). It says "has with intent or gross negligence failed to comply with regulation 72".

Stephen Jones: Yes, I have 72, which says that unless the customer has deliberately or with gross negligence failed to comply with their obligations, and then the obligations are defined under regulation 72 as X, Y and Z, but they do not actually define what gross negligence means.

Chair: It does not define what it actually is.

Stephen Jones: They say that you have to use payment instructions in accordance with the rules; you must not have handed over your personal security—

Q668 **Catherine McKinnell:** I am sorry. The rules are set by the banks.

Stephen Jones: They are not. These are regulations that are defined by European law.

Q669 **Catherine McKinnell:** I mean the rules in terms of the service use of the card. You must have that in your terms and conditions.

Susan Allen: Yes, we do. This is to keep your PINs and passwords safe and not to hand over codes, et cetera.

Q670 **Catherine McKinnell:** I do not have your terms and conditions here, but

I do have the regulations that say that this is the reason banks would give not to pay out or be obligated to pay out to a customer in the event of a fraud or gross negligence. I am just trying to understand how you apply the concept of gross negligence within your decision making, because it is down to your individual decision making. That is what I understand. I will come to my next question now, which is this. Is this applied consistently across the board? The point is that I presume it is not.

Stephen Jones: That is a fair part of the question, which is why the code will be extremely helpful. The code will set out, in much clearer terms, the expectations required of customers by the system. The third sector has signed up to this. They are not too high, but it sets out, "These are the things you must not do. If you have done this and you fall victim to authorised push payment fraud, you will be reimbursed". I have to say that these obligations we are discussing often apply in the context of unauthorised fraud as well, which is different and a much bigger problem. For the vast majority of unauthorised frauds, not where the customer has given an instruction but where money has ended up being debited from their account, they are reimbursed. The problem of customers not being reimbursed in unauthorised fraud cases is very, very small.

Q671 **Catherine McKinnell:** That is an answer to my first question, which I am going to come back to. At the moment, there is no code of practice. At the moment, each of your institutions has to apply what it deems to be gross negligence and therefore they are not obligated to refund an unauthorised or an authorised payment. I am sure you will be writing to customers and telling them that you will not be refunding them this money due to gross negligence. Presumably, you need to specify that when you notify customers that is the case.

Chris Rhodes: In our case, it is very simply that, if you disclose your PIN or are negligent in how you hold that PIN so your debit card can be used to initiate a payment, then you will be liable.

Q672 **Catherine McKinnell:** What do you mean by that?

Chris Rhodes: We see some customers write their PIN down on the back of their debit card; we see customers put their debit card in their wallet and have their PIN on a piece of paper. We see customers give their debit card and PIN to flatmates. If you do that and your debit card and PIN is used to authorise a payment, you will be liable for the loss. However—if you do not mind, I will go back to my other example, because it is really quite important—if you are duped into giving your security details away, so in our case that would be if someone phones you up, challenges you to put your debit card in your card reader and give to that fraudster those one-time passwords that will then allow them to send a payment, you will not be deemed liable; you will be refunded in that case, because you do not know what is going on. You are being scammed by a very sophisticated criminal. That is not negligence on your part, because you do not know what is going on. If you give your PIN and password away,

we would all accept that you have kind of left the keys to the house on the street.

Q673 **Catherine McKinnell:** Do you have some discretion that you can apply? We have taken evidence about a lady who was blind. She goes to pay for a taxi journey and the contactless system does not work, so she has to hand her card to the driver and get him to put the PIN into the machine. Presumably under your general definition, that would be gross negligence.

Chris Rhodes: We have a vulnerability policy, and cases are assessed on a case-by-case basis. Therefore, there is a blank and then there is your specific circumstance of vulnerability, which we would always take into account.

Q674 **Catherine McKinnell:** That is where we get into quite complicated territory. Part of our inquiry is about how you define "vulnerable".

Chair: That is a different inquiry.

Catherine McKinnell: The example you give about the phone fraud is reassuring, because sometimes you might be vulnerable to financial fraud simply because you are distracted, busy or you are doing other things. Somebody phones you and you do something, and then afterwards you think, "Oh my goodness, I cannot believe I did that", but it might be too late. Anybody can be vulnerable in that circumstance. There are other definitions, which we are looking into. We are looking into how you define vulnerability within the financial services sector.

Chris Rhodes: Vulnerability can occur at any point in time to anybody, depending on their exact circumstances.

Q675 **Catherine McKinnell:** Okay, so the answer to this is that we do need more consistency. We do need it to be applied and we need it to be better defined within the code of practice.

Chris Rhodes: Yes, which the code will do.

Stephen Jones: On vulnerability, the code will say that even if the customer has not adhered to the standards of care required by the code, if they were vulnerable they will be reimbursed. There is still a subjectivity around the definition of "vulnerable". To Chris' point, it is pretty hard. It is hard to codify, in a way that does not change over time, what vulnerability is. You may be able to come up with some examples, but it is quite hard to be completely definitive about what vulnerability is.

Q676 **Catherine McKinnell:** What about the definition of gross negligence? This is not just negligence; this is gross negligence within the regulations. There is a difference.

Stephen Jones: The code will define what is expected of consumers in order for them to be deemed to have done what is required of them.

Q677 **Catherine McKinnell:** Could you give examples of what would constitute

gross negligence?

Stephen Jones: Yes, anything that would constitute a failing under the code such that they would not be entitled to reimbursement. Gross negligence is—

Q678 **Catherine McKinnell:** Gross negligence is what is in the regulations. Financial institutions are required to explain what that means in practice.

Stephen Jones: The code we are talking about is dealing with authorised push payment fraud. Most of the rules we are talking about under the payment services directive are for unauthorised fraud. We just need to be careful about not conflating the two.

Q679 **Catherine McKinnell:** The code of practice will not actually resolve this issue, then.

Stephen Jones: It cannot. The interpretation of gross negligence, to the extent that there is no statutory definition, becomes a matter of common law. When the FOS look at the concept of gross negligence, they apply a judgment every time in terms of what they think is fair and reasonable. It is a matter of interpretation and practice.

Q680 **Catherine McKinnell:** The challenge for consumers is that they need to know.

Stephen Jones: I understand that, and so we need to do a better job of giving examples of what is and is not practice. Again, in our experience, vulnerability practice is best dealt with using intelligent discretion.

Q681 **Catherine McKinnell:** Do you mean in terms of vulnerability?

Stephen Jones: Yes.

Q682 **Catherine McKinnell:** I am not speaking specifically about vulnerability. It does appear that you have a way to address that with some discretion.

Stephen Jones: Yes.

Q683 **Catherine McKinnell:** The issue is for ordinary customers to understand and for banks to be open and upfront about what gross negligence is. It is about not being subtle and not to not wish to cause offence but still not actually refund the customer. You need to be open about what this means.

Stephen Jones: To repeat, while the regulation in question does not define gross negligence, what it does say, under regulation 72, is what the customer obligations are. It says that you have to "use the payment instrument in accordance with the terms and conditions". Yes, you have to understand what the terms and conditions are.

Q684 **Catherine McKinnell:** That is what I am talking about. The banks need to explain in black and white what they deem to be gross negligence under their terms and conditions.

Stephen Jones: You have to keep your personalised security features safe. We have talked about that. Chris has talked about that. The Take Five campaign is the industry's attempt, with the Home Office, to make sure everybody understands you should never, ever, not even to your bank, hand over your digital credentials, because you are placing your security at risk if you do that. You should also notify your provider promptly if you lose your card. That is it, actually. It is not much more complicated than that, but I agree with you: we need to bring to life what using your payment instrument in accordance with its terms and conditions actually means.

Q685 **Chair:** I am going to bring in Steve, who is going to talk about something slightly different, but on those last points we have heard evidence, particularly in relation to TSB, where customers had been taken advantage of. We know the fraudsters piled in while the IT upgrade had gone disastrously wrong. We know of customers who were told they have been grossly negligent without any investigation whatsoever. Would you agree this goes back to what Charlie was saying? If the bank for whatever reason decides that somebody has not looked after their details sufficiently, customers have to have somewhere to go to in order to get that investigated. Your view is that the FOS is the best place to go.

Stephen Jones: If they cannot agree it with the bank, yes.

Chair: Yes, the FOS is then the next port of call.

Stephen Jones: The FOS will apply its discretion in interpreting gross negligence in a "fair and reasonable" way and, I would say, impartially. It is therefore an appropriate place to go.

Q686 **Mr Baker:** Good morning. I do not think any of us have a reputation for great sympathy for financial institutions, and I certainly do not want to start a precedent, but are you not the victims of fraud as well?

Chris Rhodes: It is a huge cost to the system. Yes, we probably are, but the reality is that society is the real victim here because of the costs that flow out to criminals.

Q687 **Mr Baker:** When we were talking earlier about who should pay, really it is the fraudsters who should pay by reimbursing plus criminal convictions. What more can you do to identify these fraudsters, track where the money has gone and make sure they are brought to justice?

Susan Allen: We are investing heavily in this. As I already mentioned, we invested £100 million last year in financial crime. We have dedicated teams looking at financial crime and fraud risk. I actually went out a few weeks ago to sit with our team in Milton Keynes who do some of the fraud analytics. Honestly, although I had a good idea of what they were doing, I was frankly blown away by how clever the techniques are that they use to try to map where payments have gone. If we see a fraudulent account, the level of detail is such that we look at the device that was used to access that account, and then we look to see whether that

device, the mobile phone or computer linked to that account, has been used on any other account on our network. Where we see fraudulent accounts, we then pass that information through Cifas to the other banks, to make sure they also have that insight and intelligence.

There is a lot that we do. All of us invest significantly in trying to detect fraud. The challenge is that the fraudsters are also very sophisticated. They have a lot of money too, and they are investing. We have to keep investing to stay on top of this and to try to stay ahead of them, or at least with them, to try to protect our customers as best we can.

Q688 **Mr Baker:** Are enough people being brought to justice for all this investment that is being made?

Stephen Jones: No. The financial sector spends about £5 billion on aggregate in the UK on the fight against economic crime. That includes money laundering, as well as the kinds of consumer and SME fraud we are talking about today. If we take, for example, a previous thing I have discussed with the Committee, the SARs regime, which was designed to stop money laundering, it is really not very effective. Some 460,000 SARs were filed last year and you can count the number of investigations that the authorities are able to follow through at a couple of hundred, basically.

Q689 **Mr Baker:** I need to get onto my allocated questions about fraudulent bank accounts, but where within the machinery of the state would you want to see more investment made in order to improve our capacity to bring fraudsters to justice?

Stephen Jones: We have some key asks. Thank you for asking. First, we want improved information sharing. We have previously asked Government for a new power to share information more widely across the sector and not to have to have a criminal burden of proof before we start to do that. That will enable us to track, trace and prevent in a much more effective way. It could also be transformative in terms of responding to data breaches. If TalkTalk goes down again, the banking sector needs to know the next day, and it needs to know the accounts, the data and the individuals who have been compromised, not months later, which is currently what happens, depending on where the data breach has been perpetrated.

We need regulatory comfort for firms when they are seeking to slow down, when they are putting grit in the system and going against their obligations under the payments regulations to make a payment in accordance with the customer mandate. We need to know the regulators are not going to prosecute the banks, and we do not know that at the moment. We have a project going called project freeze, where we are experimenting with different scenarios where we slow down or block payments. We are doing that in breach of our regulatory obligation to make payments with no regulatory comfort in doing so, in order to try to stop economic crime. We would prefer that to be a better worked through

scenario agreed with the regulator that makes it clear that we are entitled to do that if there is a genuine suspicion and we are trying to stop fraud.

We want to make it easier to repatriate funds using technology. To your earlier observation, Steve, that the money ends up with the criminals and therefore we need to get the money back from the criminals, it is not that easy to get the money back from the criminals. We are improving the technology. We have a big pilot with Vocalink at the moment, which is enabling us to move as fast as the money moves across multiple accounts. It is often split very quickly and very intelligently in seconds and put into multiple accounts that sometimes go cross-border. We think we can track that now, but once we find where it has gone to we cannot get it back. We need to work with law enforcement, at least in this country, to the extent the money is still in the UK, and regulators in order to enable that to happen.

We need to be able to unlock suspended accounts. There are hundreds of millions of pounds that are blocked in banks as the suspected proceeds of crime that are just frozen. Nothing is happening to them. There is no prospect of those accounts being investigated, but they are frozen and everybody is looking at them saying, "What are we supposed to do with this money?" That money could provide an awful lot of oil in the system.

Q690 **Chair:** It could recompense people, presumably.

Stephen Jones: It could recompense as well. For example, it could seed the "no blame" pot we were talking about. We have raised that with the Home Office, the National Crime Agency and the Payment Systems Regulator, and they have said no.

Q691 **Chair:** Why did they say no?

Stephen Jones: Because they have earmarked the funds for other purposes. Finally—we have talked about this as well—we need to find a more coherent way of sectors and regulators of those sectors working together to attribute blame, because ultimately data breaches in other sectors are a significant cause of the issues that may or may not lead to victims of fraud through the payments system. The fact is that we need to work, and are working, with Ofcom. The telecom sector is very vulnerable. There are lots of security improvements that could be made in that sector that would help victims and help the banking sector in reducing the incidence of fraud, for example.

Mr Baker: That is great. I am glad I went off brief and asked, but I had better get back to fraudulent bank accounts.

Stephen Jones: I can write back with those specific recommendations, if that helps.

Chair: That is obviously very helpful to the report. Wes might pick up on a couple more, but yes, that is very helpful.

Q692 **Mr Baker:** We have been told that students might sometimes open bank accounts legitimately but then subsequently offer them for use for fraudulent purposes. This is apparently described as being a money mule. How big a problem are money mules, Ms Allen?

Susan Allen: We think it is quite an issue. We close about 900 accounts every month that we think are suspected money mules. This is a big issue. Again, it is broader than banking; it is a society-wide issue.

Let me tell you about a couple of things I have seen recently. We have had to work with Facebook because we have found ads advertising that people would get up to £1,200 by allowing their accounts to be used. Often, the victims do not understand the implications for them and what it means for them. If their account is fraudulent, they can be blocked in terms of getting future banking facilities. In that case, we worked with Facebook to get those posts taken down.

We also did some research with 18 to 25-year-olds. We found that 85% of young people in that age group have shared information on social media and online that make them vulnerable to being victims of scams themselves. We also found that four in 10 have shared their passwords with friends or family members. As Stephen referenced earlier, we think this is a population that is very digitally savvy but it is actually a population that we need to work with and educate. We have done a couple of very specific initiatives, one using a celebrity from "Love Island", which we thought would help in that target market.

Chair: Do not ask us who they are.

Susan Allen: No, I did not particularly know, but I knew a banker on the video clip would not have worked very well. We have used clips like that to try to get videos and messaging into the universities we work with and into schools. This is actually a really important issue. The impact on the victims of money mules is clearly devastating in terms of the people who are subsequently defrauded using those accounts, but the impact on the young people, who are also victims in falling vulnerable to the scammers, is also quite profound. This is an issue we need to continue to work on. As I say, we close 900 accounts every single month that are suspected money mules.

Q693 **Mr Baker:** Ignorance is no excuse, because if it was an excuse everyone would plead it. You are positively reaching out to young people to explain to them that this cannot be done.

Susan Allen: Yes. As I said earlier on, we focus quite a lot on education. We focus on what happens to customers once they have been scammed, how we support them in that process and how we work with them, but we think it is also really important to focus on avoiding these situations in the first place. Working with different groups to help to educate people is a real part of that.

Stephen Jones: We ran a campaign last year called Don't be Fooled, targeted specifically at university students as an industry to raise the spectre and explain the consequences of this. If you allow your account to be used as a money mule account, you can have real problems for the rest of your life accessing the financial system, because it is a criminal offence.

Q694 **Mr Baker:** I am going to ask Mr Rhodes in a moment, but presumably the banks are all still furiously competing for student business on the basis that people are not very good at changing their accounts. In the course of competing for that business, Mr Jones, could the banks make sure they take that opportunity to educate people about how they use their account?

Stephen Jones: Yes, and I am sure that there are individual measures that are in place to help young students as they arrive on campus to understand how to use their newfound financial freedom responsibly.

Q695 **Mr Baker:** Mr Rhodes, what is Nationwide's view?

Chris Rhodes: Again, we would agree that mules are a very important issue, because they are the accounts which receive the fraudulent funds. In terms of where we see mules, like Santander we close around 6,000 accounts a year where we think they are going to be used for fraudulent activity.

What is really quite interesting is that when you apply for an account, we check you through credit bureaus and through the fraud database. If you are not very visible electronically, so you are not on the credit bureau with a detailed record, then you have to produce paper documents. You find that those accounts that subsequently go on to become mules tend to be through the paper process rather than the electronic process, where someone is well established at an address with multiple products. Those documents tend to be genuine, and then subsequently, as has been described by Susan, the accounts then get used for fraudulent purposes. We have a whole range of monitoring in place to try to close those accounts before they ever get used for that purpose.

Stephen Jones: It is quite hard, under the new payment accounts directive, to reject an account. The customer has the right to have a bank account, and the number of circumstances in which you can reject is prescribed very narrowly. We need to be a bit careful about that. In 2017, there were 1.15 million account-opening attempts that were rejected for financial crime-related reasons, but the payment accounts directive will make that smaller, if we are not careful. There is a tension here, as Chris and Susan have pointed out, between making a judgment and letting bad actors into the system.

Q696 **Chair:** Yet we hear of whole sectors—pawnbroking being one, for example, or politically exposed persons being another—where people are finding that they are being rejected.

Stephen Jones: You hear a lot about it on the Westminster estate, I know, because it is often the biggest thing in MPs' postbags that we hear about, which is people who are connected to you having difficulty opening bank accounts.

Chair: Yes, it is money transfer services and that sort of thing. It is whole sectors. That is interesting.

Mr Baker: I am going to resist the temptation to talk about pesky Brussels rules.

Chair: That is a good idea.

Q697 **Mr Baker:** Can you just tell us a bit more about this tendency? Can you put any statistics around this idea that these accounts tend to be opened through paper identification?

Chris Rhodes: I do not have that. I can clearly write to you with a profile of what we see and how many there are, yes.

Q698 **Mr Baker:** We have talked about accounts being opened by legitimate students and then becoming fraudulent accounts. What is the scale of the problem of accounts being deliberately opened as fraudulent accounts from the off? You mentioned accounts opened with paper ID that subsequently become used for fraudulent purposes. What is the extent of the problem where they are opened from the very beginning for fraudulent purposes?

Chris Rhodes: I would say very few. It is where the paper is fraudulent. Clearly, we do not know it is fraudulent; otherwise, we would not have opened the account in the first place. It does appear in most cases that it is accounts that subsequently turn out to be used for fraudulent purposes, where those people really do exist at the address they said they were living at. Those accounts are then used for fraud, rather than it being a fictitious person.

Susan Allen: It can sometimes be that accounts are opened and they actually look perfectly normal for years and then something happens. Obviously, we use detection, but they are quite tricky to spot.

Q699 **Mr Baker:** Do you think social engineering is being used to draw people into money laundering? Is that what this amounts to?

Stephen Jones: Yes, absolutely.

Chris Rhodes: They are being duped.

Q700 **Mr Baker:** What should people look out for? What is the route in for a fraudster to persuade somebody to get involved with money laundering? We are accustomed to talking about the mechanisms of APP fraud, but what is the mechanism by which a person is approached to be drawn into using their account for money laundering?

Stephen Jones: It is advertising on social media that is offering money for nothing, basically: "Let us use your account to process a few payments". It is the classic letter you get from certain African countries. It is pretty visible, but you have to educate people about it. It does change; how they do it changes. We need to ensure that we remain vigilant and that we continue to educate people about what to look out for.

Q701 **Mr Baker:** Did you want to add something?

Susan Allen: No, I would agree. The Facebook post is one example, where they were offering £1,200 for doing nothing, for allowing things to go through your account. There is a big education piece. People do not understand what that means. Actually, this is not just some sort of a basic scam. This is facilitating money laundering, economic crime and serious terrorism. We have to do a lot more on education.

Q702 **Chair:** How helpful were Facebook? How prompt were they?

Susan Allen: Yes, we found them responsive.

Q703 **Mr Baker:** You mentioned closing 900 mule accounts per month. Overall, how many fraudulent accounts a year are you closing?

Susan Allen: We close about 24,000 accounts every year. These are accounts that were in operation that we then have suspicions about. Obviously we have to have a firm reason to close an account. We cannot just close an account on a whim.

Q704 **Mr Baker:** Forgive me, but how many accounts do you have at the bank?

Susan Allen: We have 14 million, although that is a stock.

Q705 **Mr Baker:** How is this number changing over the years?

Susan Allen: I do not have the data with me in terms of the closure rates over the last few years, but I am happy to provide it afterwards to the Committee, if that is helpful.

Q706 **Mr Baker:** That would be great. Thank you very much. What about Nationwide?

Chris Rhodes: We close about 12,000 accounts. We have about 7.5 million or 7.7 million current accounts. Again, I do not know what the trend has been historically. Again, I can let you know.

Stephen Jones: The FCA may aggregate the data. I will try to come back to you with the industry aggregated data that the FCA has.

Q707 **Wes Streeting:** I will be on some similar terrain. First of all, I should just point out, following the scenario that Catherine discussed in terms of the situation with the blind woman in the taxi, that she was not a victim of crime in that case. As chair of the all-party parliamentary group on taxis, I just wanted to make that clear.

Chair: Absolutely, yes. The driver was very trustworthy.

Wes Streeting: Taxi drivers are as honest as the day is long. Anyway, I will go back to my questions. I will start with you, Stephen Jones. You have previously suggested some form of levy on payment transactions to pay out on "no blame" scenarios. I wondered whether you could describe how you envisage this working in practice. Would it be part of regulation or legislation? How would it work?

Stephen Jones: In terms of getting the APP CRM code up and running this year, the banks that are party to the steering group have agreed that they will fund that by way of an initial contribution in order that customers who are not to blame in circumstances where the banks are also not to blame nevertheless get reimbursed, but with a view to developing, with the Payment Systems Regulator and Pay.UK, a longer-term funding mechanism. We have all talked about the principle of insurance, which might underpin that mechanism, but we have not determined yet through the steering group ultimately, with the Payment Systems Regulator and Pay.UK, what the right mechanism might be.

I am afraid I cannot answer your question directly in terms of what the long-term mechanism might be, but if one looks at the concept of insurance, it has an element of payment, mutualisation of risk and an element of responsibility of each of the individual participants within that system. If you leave your keys in your front door on your way out and you are burgled, your insurance policy might not be valid. That is the kind of example that one would use to bring to life what consumer responsibility in the payments system is as well. They will get paid if they have done what they are supposed to do. What they are supposed to do is not that hard, but, if they fall below the standards that society judges reasonable and are not vulnerable, they may not have access to the funding.

Q708 **Wes Streeting:** I am interested in the evolution of the language in the approach from "levy on payment transactions" to now being couched in the insurance principle. I appreciate your candour that this is something that requires further thought and consideration. Could you just elaborate a little bit on how those discussions are playing out? What was the industry response to the suggestion you floated? What are the kinds of factors that are being weighed up? What is going to frame the discussion you have in terms of determining the right way forward?

Stephen Jones: There has been quite a lot of discussion at the steering group, and I do not personally sit on the steering group. It comprises representatives from the banks and the third sector and it is chaired by Ruth Evans, with support provided by Richard Lloyd. They sit on the steering group and they could provide perhaps a more accurate genesis of the thinking. As I understand it, the thinking has evolved. Initially, there were several months of discussions about whether the banks should be responsible in all circumstances. The parties came to the view that it was not appropriate and that shifting liability onto the banks in all cases

was not the right thing to do for reasons we discussed earlier in the Committee. Then the difficult question becomes about what alternative sources of funding there are. I have cited one, which we looked at, which is looking at frozen bank accounts that have been frozen because they are suspected to contain the proceeds of crime. That is not within the control of the banking sector, and the public authorities have said that those accounts will not be available for the purposes of funding "no blame".

One does have to work one's way through what the available options are and what the fairest way of sharing the cost is. If I can use a crude expression, we need to make sure everybody has skin in the game. It is really important that society at large understands what the cost of fraud is and understands what the cost of insuring this "no blame" pot is. With that visibility comes measurability. We can measure how effective we are as banks, working together with the Payment Systems Regulator to try to reduce the overall scale of the problem. We can also judge the extent to which consumers are stepping up and doing better in response to our efforts to educate them to reduce the incidence of fraud where they have fallen below the requisite standard of care that is required of them. At the moment, that is the stage we are at.

We are edging forward to trying to figure out what the overall size of the pool would be. I gave you a number of about £30 million to £40 million for "no blame, no blame" estimated for this year. We also need to figure out how one might fund that in the least unfair and most shared way. There is an acceptance at the steering committee that there needs to be a cost borne by both the banks and the consumers. The cost of funding that pool needs to be borne by both banks and consumers, which is an important principle as well. Both sides have to have skin in the game in that context, but beyond that we have not gone any further.

Q709 **Wes Streeting:** I would like to invite other members of the panel to give us a bit of a steer on the thinking and some of the issues that will be kicking around as the industry follows the path Stephen has outlined.

Chris Rhodes: There is not a huge amount to add to what Stephen has said, other than that the scheme needs to be sustainable. Particularly, it needs to make sure it can fund the "no blame" cases. It needs to have choice in there. I do not think every institution would necessarily want to charge their customers. Some clearly may. Our position would be that we would not charge our members for the insurance scheme, but it should be down to each individual institution to make that call. It needs to be sustainable and reflect everybody's responsibilities.

Q710 **Chair:** Can I just intervene there to check something? You are basically saying the banks on the steering group have agreed to fund this in the early years, but neither Santander nor Nationwide is on the steering group.

Chris Rhodes: Yes, we are not actually on the steering group, I do not think, but we will fund.

Q711 **Chair:** Once the steering group has reached a decision, everyone is going to be part of the scheme.

Chris Rhodes: We are engaged in all of those conversations, and we will absolutely pre-fund and absolutely sign up to the code.

Q712 **Chair:** Is it the same for Santander?

Susan Allen: Yes, it is similar for Santander and indeed other banks were in a meeting just last week on this. We fully support the code, and we are working through all of the standards. This is an issue for all of us. When you see some of these "no blame, no blame" cases, they are incredibly difficult. I am sure you see many from your constituents. Judgment has to be exercised. We have senior teams who look at all of these cases. We think that having an appropriate way of refunding those consumers in "no blame, no blame" cases is really important.

Q713 **Wes Streeting:** In terms of the regulatory and legislative frameworks we have now, are there areas where Parliament needs to look to improve the framework you are governed by? We do not often have people queuing at the door from different industries, particularly yours, saying, "Put some more regulations in place", but I am curious.

Susan Allen: Stephen summarised this really clearly earlier on. All of us would fully support the points he made.

Stephen Jones: It is very unusual for us to ask for regulation. There is no question that liability, in the context of victims, is a really difficult thing, but we are doing the best we can on a voluntary basis to make sure that happens.

Q714 **Wes Streeting:** That gives me a bit of time to touch on another issue, which is identity fraud. How well is the industry tackling this issue? Do you want to speak for the industry, Stephen?

Stephen Jones: I can start in terms of what we are trying to do. Chris has talked about some of the issues with identifying individuals as they seek to open and enter the financial system and what is being done about it. From society's perspective at large, there would or could be significant benefit to a greater public-private coming together around electronic ID. I am not trying to make libertarian or non-libertarian comments about whether we should be carrying ID cards.

Chair: Steve's head immediately went up.

Stephen Jones: Yes, I saw the head go up, Steve. There is no question that there is a social value to coming together to identify how better we can all prove our identity in a manner that is simple and effective and how that proof of identity can help us access financial services, government services and utilities services, but getting everybody around

the table to try to do that is quite hard at the moment. We are trying, and we are trying with a number of the larger financial institutions to run a pilot in terms of assessing what a use case would be for a shared form of identification that enables simplified onboarding into financial services, but it will not work for financial services on its own.

For that onboarding to be really compelling for a customer, it needs to help them onboard to DWP, HMRC, British Telecom and their gas supplier, as well as their banks and their credit card providers. As a sector, we are looking at it. We are actually spending quite a lot of time on it. Where we look at examples of this working successfully in other jurisdictions, it has required absolutely hand-in-glove public-private partnership, and we are not seeing that in the UK at the moment.

Q715 **Wes Streeting:** I have just opened up a whole can of worms. We could do a whole session on this. I cannot do another round of arguing with Steve about something else.

Just thinking for the moment about the framework we currently have, I always think the proof of the pudding is in the eating. I was a victim of identity fraud. One of the things I found pretty shocking was the variability of banks' customer service in trying to report the fraud and have it dealt with but also how negligent some of the lenders were in providing credit cards and bank accounts when information provided on the fraudulent application was markedly different from the information that banks would have had access to through the credit reference agencies. Happily for Susan, while Santander was one of the lenders that gave out a credit card, the good news was that your customer service was excellent, so lucky you.

Chair: I am sure you are relieved to hear it.

Wes Streeting: It is lucky Barclaycard are not here, because in their case, I found the reporting of the fraud as pleasant as pulling out teeth and I also found it shocking that, as an existing Barclaycard customer, Barclaycard lent a new card with a spending limit of thousands and thousands of pounds when they ought to have known, as an existing customer, that I did not live at my old address anymore. They seemingly did not even do a credit reference check. There were other examples where the address was obviously wrong. In one case, I lived at the address longer than the address had existed. I thought this was really basic stuff. You are right about the costs to banks, the industry, consumers and society at large, but, looking at this, I thought this was pretty ropey practice. I think I am right. Do you?

Chair: Discuss.

Susan Allen: Interestingly, I was also a victim of identity theft fraud in the middle of last year. I had accounts or credit cards set up with a number of other organisations in my name. What I would say is that, first of all, the response from Santander was excellent, as I would expect.

Stephen Jones: As a customer, I am delighted.

Susan Allen: I have to say that the other banks were also responsive. Knowing how the processes work, I also asked quite a lot of questions about how those accounts had been opened. The reality is that every bank will make risk-based decisions based on various parameters and various filters when they are opening accounts. Everyone will be different. They will be looking at the things they think constitute risk. There is a balance between ease of opening for consumers and the level of checks and processes you go through.

What I would say in all cases is that after the marker was placed on the account—this is the Cifas marker that will be placed on your account when there is a fraud—there has not been any reoccurrence. The industry works together very well when there has been an incidence of fraud to report that, get that Cifas marker on the account and preventing further action. Although it is not great when it happens to you, the response was excellent. I would feel very confident that the banks operated together to make sure that was closed down.

Q716 **Wes Streeting:** That bit does work well, the part after the event. It was the judgment that led to lending thousands of pounds in my name on inaccurate information that I found pretty poor. Chris, do you want to come in as well? Given your seniority in the organisation and where you sit, to what extent do you actually pull up the bonnet sometimes and look at systems, processes, the technology or the information that is available and make sure you have not just people but algorithms that are doing appropriate checks and flagging early on suspicious information or inaccurate data that might suggest this is fraudulent?

Chris Rhodes: From our point of view, identity theft is not a huge issue. Therefore, the customer service, as has been described, when it does happen, is incredibly important. It is difficult to comment on other people's matching systems, but you would expect what is on your application to match. Of course, there might be multiple records at the bureau. I could be Chris Rhodes, Christopher Rhodes, Chris S. Rhodes, but the matching algorithms should be able to pull that out.

We find the weak link is actually the postal system, because there is enough data in the public domain, certainly for many of us in this room, to be the victim of identity theft. It only really then happens when someone can intercept the card, the chequebooks and the things that go out to make the account operational. There should be more of a focus on making sure the postal system is really secure. Ultimately, that is our test of whether this is the person. We are pretty sure they have all the data. If the address does not match up, I do not quite know how they got to that point. We then post it, and of course they cannot do anything with that card unless they can intercept the post coming to your postal address. From our point of view, we see that as the weak link in the process.

Q717 **Wes Streeting:** Stephen, is there anything you want to add on behalf of the industry?

Stephen Jones: As has been pointed out, once the fraud has happened, the various measures and bodies that exist are pretty good. There is the national fraud intelligence bureau, Cifas, which Susan has mentioned. We run the Financial Fraud Bureau, underneath which is the financial information-sharing service. Our ability to join all the dots together across the system is pretty good. I have seen AI at work in the customer databases of members, including those around the table, the applications of which are incredible and which prevent really serious harm.

There are good things that go on, but I accept that the onboarding standards do vary. They are individual risk-based judgments that firms make. I am aware of one firm that will open a payment account automatically if you have a bank account with one of the big five banks.

Q718 **Wes Streeting:** Do you want to tell us who they are?

Stephen Jones: No.

Wes Streeting: I thought so.

Stephen Jones: So there is no question that standards are variable, and we need to think about what that means.

Wes Streeting: All I would say is that the last set of figures on this I saw suggest that Cifas is sending something like 800 cases of identity fraud to the police every day. This is clearly a significant area of economic crime. The industry just needs to reassure itself that it is doing everything it can to mitigate at the initial stage, not just what happens when things go wrong. In terms of customer call handling, when a customer asks for an explanation as to how it was, as in the case in Barclaycard, that one of their customers was done over to the extent I was, it is probably best to make sure that complaint is followed up, because—you never know—they might be on the Treasury Committee and might raise it publicly in this forum. Who knows? I might actually get the letter I asked for all those months ago.

Q719 **Chair:** They might be watching. I just have two final questions on an area we have already touched on. Both are about information-sharing. One is about your relationship with the police. You have talked about sharing information with the police. Does every incident of economic crime and suspected fraudulent behaviour get reported to the police? Do you have any internal thresholds that have to be met before an incident is reported?

Chris Rhodes: Every case of scamming and push payment fraud we would submit to the NCA. All of that is reported. The element that is not reported but is captured in the industry statistics we send to UK Finance is cardholder-not-present fraud, where we clearly know who the victim is but in most cases we have no idea who the perpetrator of that fraud is. All of that data is available to the dedicated police unit, but we actually do not report individual cases of cardholder-not-present fraud.

Susan Allen: We are the same.

Q720 **Chair:** Secondly, we have talked about things you want to change. I just wonder how GDPR perhaps affects this. Mr Jones, you might answer. Has the general data protection regulation helped or hindered information sharing?

Stephen Jones: We do not think that the criminal exemptions provided by the Data Protection Act are clear enough to support information sharing at the required speed and scale. We proposed to Government a general power and safe harbour for banks to share information for the purposes of preventing and detecting all types of economic crime. We asked for that in the Criminal Finances Act, and indeed the FCA supported that call, but Government rejected it.

Q721 **Chair:** On what grounds did they reject it? No answer came there.

Stephen Jones: We are not quite sure.

Chair: That is another good one for our report. Thank you very much. Can I thank you all very much for being here this morning? I know that preparing for evidence sessions takes some time, so we are really grateful to you for your presence here this morning and all the answers you have given. There is some more information to come from various sources, but thank you all very much this morning.