HOUSE OF COMMONS

Treasury Committee

Oral evidence: Economic Crime, HC 940

Tuesday 27 November 2018

Ordered by the House of Commons to be published on 27 November 2018.

Watch the meeting

Members present: Nicky Morgan (Chair); Colin Clark; Mr Simon Clarke; Charlie Elphicke; Catherine McKinnell.

Questions 514 – 563

Witnesses

I: Richard Piggin, Head of External Affairs, Which?, Richard Emery, Independent Fraud Investigator, 4Keys International.

Written evidence from witnesses:

– Richard Emery, ECR0077 and ECR0076. Richard Piggin, ECR0044

Examination of witnesses

Witnesses: Richard Piggin and Richard Emery.

Q514 **Chair:** Good morning. Thank you both very much indeed for being here today for this next session in our economic crime inquiry. I will ask you to introduce yourselves and then the Committee members have a series of questions. Mr Emery, I know you have sent in some written evidence as well, ahead of the session, so thank you for that. Perhaps we can start with you. Can you introduce yourself for the tape?

Richard Emery: My name is Richard Emery of 4Keys International—it is a sole trader arrangement, so Richard Emery and 4Keys International are synonymous. My career background, very briefly, is that I originally trained in accountancy and then went into computing. I worked for John Lewis Partnership on the whole design and development of point-of-sale and payment systems. I worked for ICL Retail Systems, again in retail inventory management systems. I established my own consultancy 30 years ago and gradually moved into the area of working as an expert witness in fitness for purpose of retail computer systems. Then I moved into the area of criminal defence for people accused of retail theft and fraud, credit/debit card fraud and bank fraud. For the past six years I have focused primarily on assisting individuals who have been the victims of fraud and are challenging their banks. I currently have just over 80 cases on my desk totalling some £2.6 million.

Chair: We will come back to explore some of that, so thank you very much indeed.

Richard Piggin: My name is Richard Piggin. I am head of external affairs at Which?, which is the largest consumer organisation in the UK. We regularly hear from members, our supporters and members of the public about their experience of fraud. In particular, we have focused on the issue of authorised push payment fraud, which I am sure we will touch on later, where we think there have been some significant failures and a lack of protection for consumers that has resulted in a significant amount of harm.

Q515 **Chair:** We are definitely going to return to authorised push payment fraud, but I want to start with the other types of consumer economic crime that you see. Mr Emery, without going into details, if all the cases on your desk do not just relate to authorised push payment fraud, can you tell us what else you have on your desk?

Richard Emery: The cases on my desk divide into three piles. As you have identified, one pile is push payment fraud. One pile is accusations of gross negligence, where the individual has effectively allowed somebody to access their bank account, the fraudster has taken the money from the bank account and therefore the transactions were unauthorised, but the banks have said that the individual has been grossly negligent.

I have worked very happily with the Financial Ombudsman service over the past year. In August, the Financial Ombudsman service indicated that it is raising the bar for the standard of gross negligence. It is now saying that if a bank wants to accuse a victim of being grossly negligent, it is a very high bar. It has issued three provisional decisions: one has been accepted and the other two are still being negotiated, but we are getting there. The Financial Ombudsman service is being very good; it is very clear now on where it stands.

The other third is a whole variety of individual cases where people have been the victim of fraud in relation to their bank and then there are different issues that have come from that. I recently assisted somebody who, nine years ago, was the victim of a physical attack and has suffered from a certain degree of brain injury. His account was recently used to process stolen money and the bank put a fraud marker on Cifas. We just heard in the last week that the bank has realised that they got it wrong and has taken the fraud marker off. Everything I am doing relates to credit/debit card fraud and bank fraud. A lot of cases have fallen around the question of who authorised the transaction.

Q516 **Chair:** That is really helpful. We are going to come back and ask you some questions later on about vulnerable consumers, and vulnerability defined by the FCA in a very broad sense, because we are doing a separate inquiry on access to financial services by customers with vulnerability. Mr Piggin, leaving authorised push payment fraud to one side, can you perhaps give us the sorts of complaints or queries that people come to you about in relation to consumer economic crime?

Richard Piggin: In the last 12 months, *Which?* magazine has published at least 15 different features and investigations into different types of fraud. They can vary from card-not-present fraud, as Richard was talking about, or unauthorised transactions, when a fraudster steals your card or banking details and makes a transaction that you are not aware of. We also have instances of identity theft, where a fraudster will steal your complete identity and open up a completely separate account, unbeknown to you, and use that to make purchases and transactions. We will see different types of fraud, so investment fraud, pension fraud and romance scams.

The concern that we have is that, for certain types of fraud, the relative impact on the consumer is not so large. With unauthorised transactions, for example, in most cases the customer, financially at least, gets their money back; they do not lose out. With identity theft, yes, they could have difficulties in applying for credit, or getting a loan or mortgage, but in general the financial harm is limited. The problem that we have with authorised push payment fraud is that those protections are not the same and the impact on the consumer is significant, because they are losing their own money, and sometimes their life savings. We cannot say clearly enough the significance of the impact of the consumer.

If you are talking about the scale of fraud, you can look at figures from Action Fraud and the Office for National Statistics. There were over 3 million cases in the last year. The UK Finance figures talk about hundreds of millions of pounds lost to economic fraud to consumers over the past year. What the statistics sometimes do not tell you is the impact that those types of fraud have on individuals, and those are the stories we hear, where the impact on the individuals from fraud is so significant.

Richard Emery: Could I comment on the unauthorised issue? I agree generally with what Richard says. Generally they are smaller amounts of money, but I have somebody sitting behind me who, nearly two years ago, lost £180,000 through unauthorised transactions and we are still in dispute with their bank.

Q517 **Chair:** With all of these things, in terms of the impact on consumers, you are right; obviously there are different scales, but these crimes are devastating. We have heard, and I am sure you have heard cases, certainly in relation to TSB when we were taking evidence on that, the experiences people shared with us of the devastation caused by watching money disappear from their bank account were heart-breaking.

I want to talk about the scale of this crime and how prevalent it is. As I understand it, UK Finance says that a total of £503.4 million was stolen by criminals through authorised and unauthorised fraud in the first six months of 2018. It also says that, during the same period, the finance industry prevented £705.7 million of unauthorised fraud. Do those figures sound right to you? How prevalent is this as an issue? You have just given, Mr Emery, a very high figure that somebody has lost. Do you have an average figure? I do not know whether Which? does, from the basis of the complaints it has. Mr Emery, do you want to go first about numbers and scale?

Richard Emery: If we are talking about authorised push payment fraud, which is the one of greatest concern at the moment, as far as I am concerned it is inevitable that the people who take the time to come and find me are going to be people who have lost more money. I would also say that, despite making a request to UK Finance, it has not revealed any detailed information of the breakdown of the 80,000 cases that have occurred in 2017 and the first half of 2018. I have been asking for that information, but that information has not come.

Q518 **Chair:** What sort of breakdown are you looking for?

Richard Emery: The breakdown I am looking for says, of those 80,000, how many of them lost £50, how many lost £5,000 and how many lost £10,000, £20,000 or £100,000. Of the 31 cases on my desk, the average value is £52,000.

Chair: That is still a significant amount of money for most individuals.

Richard Emery: Yes, and my reverse calculation on the figures that I have gleaned from various different sources tend to indicate that, of

those 80,000, a very large proportion have lost a small amount of money and a small proportion have lost an average of £20,000 each. That is a life-changing amount of money. The area I am trying to focus on is those people who have lost very large amounts of money, because it has an impact, as we will talk about later, on the way in which I believe the police and the banks should be looking at it. If there is no understanding of how the frauds are happening, and whether they are all small or large values, neither the banks nor the police are in a position to respond in the most appropriate way, and there is a serious lack of information. In my paper I have mentioned something called network-level transactional data analysis, which we might talk about briefly later on. In my experience, there is a huge range, but my figures tend to start at £10,000 up.

Q519 **Chair:** Mr Piggin, what is the Which? view on scale and prevalence?

Richard Piggin: It is going up. If you take the UK Finance figures for authorised push payment fraud in the first half of 2018, about £145 million was lost. Although not directly comparable, if you look at their figures from 2017, there is an increase of 44%. Only £1 in £5 is ever returned to the customer, so it is significant loss. The average loss depends on the type of fraud. You will get some purchase fraud, where you might buy a fake product online that does not exist. That is probably the most common of the scams, but the relative amount is less than something like invoice or mandate fraud, where there are fewer cases but the amount lost is significantly higher. Purchase fraud was £19 million across 21,000 cases in the first six months of 2017. Invoice and mandate fraud was £49 million, so that is potentially paying for a house deposit or big building work, so naturally those figures are much higher.

Q520 **Chair:** What do you see in terms of the socioeconomic divisions? Who is being targeted? Without going into specifics, what is the background of the people in your caseload, Mr Emery? Who is coming to you?

Richard Emery: As far as I can see, there is no socioeconomic pattern at all. These are ordinary people. They are people who have saved up over many years. In one case a £163,000 deposit on a house was gone. Holly is sitting behind me—I am sure she will not mind me describing her as a very ordinary person. It is that sort of situation. Equally, I am not asking the questions.

Chair: You are getting random members of the public who find you and then, presumably, come and ask for your help.

Richard Emery: They are just everybodies.

Q521 **Chair:** Mr Piggin, do you detect any particular groups or backgrounds?

Richard Piggin: There is a bit depending on the type of scam. We did an investigation into a Microsoft IT software scam and spoke to some people who perpetrated that scam. They deliberately targeted the elderly and those who were less computer-literate because they felt they were

more susceptible to falling victim to that type of scam. If you look at the crime survey for England and Wales from 2017, it shows that 14% or 15% of victims are re-victimised within a year, so there is some re-victimisation.

When we looked at authorised scams, Which? did some research into whether consumers had made a payment into a fraudulent account, and about 3% of consumers had said that, but it was significantly higher, about 8%, of 18-34 year-olds, so we found a younger audience were falling victim to that particular type of scam. Maybe that is because of social media; we are not sure. In general, I agree with Richard that, for certain types of scam, anyone can be susceptible.

Q522 **Chair:** That is interesting. Before I hand over, do you detect patterns of types of crime? Is it often people who are less IT-literate, people who are very busy or people who tend to do things through mobile phones rather than sitting at computers and thinking through what they are doing? Do you detect people who are perhaps less suspicious of the phone calls that they get and things that do not ring true?

Richard Piggin: Fraudsters will prey on the particular vulnerability and characteristics of those individuals, whether that is a characteristic such as not being computer-literate or being hard-pressed for time. We have heard of cases of people being called straight after work or late in the evening, where they are prompted or pressured into making a decision quickly. Perhaps, for example, on a Friday night they are persuaded into making a transfer because they fear that their account has been compromised. They transfer some money into another account, because the fraudsters knew that, if they then realised or were slightly worried, having thought about it for half an hour, that if they reported it to their bank's fraud team, the team might not be available 24 hours a day and it might not be picked up until the Monday morning, by which time the fraudster could have cleared the account.

Chair: How depressing.

Q523 **Charlie Elphicke:** Good morning. Just looking at UK Finance's publication on 19 November, they said that criminals stole £500 million through fraud and scams in just the first half of 2018. Is this now rising and getting out of control, Mr Piggin?

Richard Piggin: It is definitely on the rise. It is concerning that these figures are rising, even since Which? made a super-complaint on this particular issue back in 2016. It suggests to us that the response so far has not been sufficient to address the problem of online fraud. To be clear, there are challenges, but we are concerned that the response so far, particularly from banks, has been slow. Their response to date has focused very much on education and awareness-raising, which we might touch on later, and we are not convinced that there is enough evidence to show that education and awareness-raising has an impact on reducing the amount of fraud. Then we believe they have been slow to implement

certain measures that would have been more effective in preventing customer losses.

Q524 **Charlie Elphicke:** Do you think that the PSR and UK Finance prioritise protecting banks over protecting consumers and victims of fraud?

Richard Piggin: We were disappointed with the PSR's initial response to our super-complaint. We did not feel it went far enough to address the harm that we had identified. It asked the banks to go away and collect some data, improve how they respond to victims of crime and to share some best practice. It did not address the fundamental issue of where the liability sits for those losses. We were worried that far too much responsibility was placed with the consumer. We are still worried that far too much responsibility is placed with the consumer. We argued that, if you placed more liability on the banks for the losses from this fraud, you incentivise them to put in place better mechanisms to prevent fraudsters from using their bank accounts and payment systems to enable fraud.

Q525 **Charlie Elphicke:** We have heard evidence to this Committee from UK Finance that said that, rather than customers or banks taking the risk, everyone should take the risk and it should be effectively socialised as a kind of criminal tax placed on everyone. What do you think of that?

Richard Piggin: We are getting into what should happen when a customer has done everything that they could reasonably be expected to do to protect themselves from fraud and, let us be honest, that is a very high bar. We are also getting into the territory where the banks will claim that they have also done everything they can, and that is what they will claim. There is a situation where the customer has lost money but they are not being reimbursed.

Everybody agrees with the principle that, if the customer has lost money, is not at fault and has not done anything wrong, they should be reimbursed. The challenge we are getting to is who funds that reimbursement. It should not be the consumer or the customer. That is where it sits at the moment and we think that is grossly unfair. The banks will argue that it should not be the banks, so they might point to it being more of a social responsibility, as you said. Should it be the Government? You have raised before whether it should be dormant accounts, and that was quickly dismissed. We agree. We think the liability should be placed more on the banks, but there are some interesting developments that need to be considered.

For example, if a bank says that it has identified an account, not frozen or dormant, but they suspect that it is a fraudulent account, they have repatriated some funds to some victims where they have been able to, but in other cases the trace has been too difficult. It has gone through many banks and it is not clear how they could repatriate. They have contacted the owner of that account and not heard anything back, so the banks are sitting on that money. They feel that they could use that money to reimburse genuine victims who have done nothing wrong, but

there is an argument that they are fearful of acting because there is existing legislation that makes them wary of acting. For example, they do not want to handle proceeds of crime.

If that is the case, there are two things that need to be done. Banks need to be very clear about what in legislation is preventing them from acting in their best interests, preventing fraud and essentially doing the right thing. They need to make that case, and then the Government and the regulator need to look, and it is their responsibility to try to unblock some of those challenges. If you could unblock them, I do not know, but it might mean giving some banks a protection in good faith, a letter of comfort, which says, "If you do this, you are not breaching the legislation, so individuals at your bank will not go to jail." If that is what is needed and you can give that sort of reassurance, we can overcome some of those barriers.

What that needs is the banks working together, with the Government looking at it and the regulator. What we are seeing, and hopefully what we are putting across, is that this is a significant platform. It needs to be a priority for everybody; it is not just a priority for Richard, me and others. It should be more of a priority for banks and it is becoming more of a priority for banks. That is clear. It should also be a priority for the Government and the regulator.

Q526 **Charlie Elphicke:** There was a proposal, which I think came from UK Finance, that the money should not come from the customer or the bank. It should come from dormant bank accounts. To my mind, there was moral hazard in allowing the banks to steal from charities and good causes to make up for their own incompetence and failure to put systems in place. What do you think?

Richard Piggin: That is exactly right. That is why we are looking at alternative options. There are a number of options for where you could get this money from, and I think you are completely right about dormant accounts, in that they are allocated for specific good causes. The additional point to make around who should fund this and be liable is that we want to place the incentives on the right people here. If it comes from dormant bank accounts or other sources, where is the incentive on those banks to respond to future incidents of fraud? Fraud changes. It will become more sophisticated. Where is the incentive on them to adapt and improve their measures continuously? The argument of our super-complaint is, if you placed more liability on to the banks, they would be incentivised to continually improve the systems and measures in place to protect their victims. We need that incentive placed on those that are best placed to manage the risk.

Q527 **Charlie Elphicke:** Mr Emery, we have talked a lot about authorised push payment fraud, but that is not the only fraud here, is it? There are also impersonation scams. How do they work and how can they be prevented and counteracted?

Richard Emery: It is quite difficult to grasp the question of what we mean when we talk about an impersonation scam. There are a number of different ways we could define that. Are we talking about a situation where somebody consciously pretends to be me, or are we talking about somebody who pretends to be somebody who does not exist? I do not personally have any experience of the situation where somebody pretends to be me or somebody pretends to be another individual person to access their funds directly. I have significant experience of where people are opening bank accounts in names and identities that are not theirs. They are pretending to be somebody, but the somebody they are pretending to be does not actually exist.

If I could come back to pick up on something that Richard said about responsibility, I am firmly of the view that the banks should take responsibility, particularly in the case of authorised push payment fraud, but also because of the money that is received through unauthorised transfers for gross negligence. I take that view because there are three things that the banks could have done, should have done and have not done. Those three things are tied into account opening failures where they are not compliant with the money laundering regulations; transactional processing failures where they are not compliant with the payment services regulations; and a general monitoring of accounts.

When you have a situation where a student account that is operated normally for three years suddenly gets 14 payments totalling £100,000, and the banks simply allow that money to flow through, I consider that the bank has failed because it is not monitoring the activity of that account when it reasonably could have done. If a student walked in and said, "Can I have a bank account and I want to be able to process £100,000 through it?" the bank will say, "That's fine." If they walk in and say, "Can I have a credit card with a £100,000 limit?", the bank is going to say no.

The banks are not doing enough and those are three key areas where the responsibility lies. I am currently assisting somebody who is taking a case—I cannot name them because it is going through the county court at the moment, so I will be careful about what I say. The police have identified that the account was opened with fake documents and the bank is still defending the fact that they accepted money into that account. To me, that is the key.

Could I make another comment? The banks have said that there is a big issue with student accounts being used for money muling. I do not disagree with that, but I contend that the banks are not monitoring those accounts when they should have been.

Q528 **Charlie Elphicke:** Mr Piggin, the banks have come under fire for shirking their responsibility, but they then say, "We have the banking protocol. It works and has been a massive success." Are they right or is that just a cover for them being shirkers?

Richard Piggin: Banks are making progress and they have introduced certain measures and done certain things. The banking protocol is a good example of where banks have worked together with local police forces to introduce a mechanism or measure that they have now evidenced prevents fraud. They have statistics to back it that it works and prevents fraud. That is great and we would like to see more of it.

There are two things I would like to say in respect of it. One is that this is a protocol that works effectively in branch, as UK Finance shows. With the declining branch network and more customers making payments online, there is a question as to how you can adapt the banking protocol to be fit to keep pace with the changing nature of payments. How does it work in an internet or mobile banking framework?

The other is that we would like to see evidence of the impact of the other measures that the banks have introduced and are introducing in reducing fraud. We are seeing banks putting in place stricter warnings at the point of transfer, which are more personalised to the customer. That is a step forward. We did not see that before. They are putting in place other technical solutions to address the problem. We are really keen to see what impact that has and the measurement of that impact over time to show what works and what does not.

I will come back to the education and awareness-raising campaigns that you will see. Lots of banks have invested a lot of money in raising awareness of fraud. There is definitely a place for education campaigns. Which? does it; we talk about fraud in our magazine, and we give advice and information to consumers on how to spot fraud and how to help protect yourself against fraud. There is definitely a role for that. We would like to see what impact that actually has in reducing fraud in comparison with some of the other measures. We might talk about confirmation of payee, for example, and what impact that will have on preventing fraud. Then we need to focus our attention on those measures that have the greatest impact on reducing the harm on the customer.

Q529 **Charlie Elphicke:** Many of my constituents in Dover and Deal have been victims of these crimes. Since you submitted your super-complaint, what changes have there been and what changes do you hope to achieve to make sure that my constituents are no longer going to be at risk of being defrauded in this way?

Richard Piggin: Since the super-complaint we now know the scale of the problem, which is something that nobody knew before our super-complaint, even though there were cases that banks would have been aware of, complaints they would have received and cases that the Financial Ombudsman service would have received on this. We now have a benchmark of how much is lost, which is progress. We now have better reporting mechanisms. Banks have now introduced better ways of responding to victims. I mentioned the fraud line closing at 5 o'clock on a Friday and opening at 9 o'clock. We are seeing much more of a move

towards a 24/7 fraud hotline nature, which is what is needed, so we are seeing progress.

There is still a lot to be done. I represent Which?, but you might be aware that I am also part of the APP scams steering group that is responsible for developing a code that would give reimbursement to victims of APP fraud. I cannot speak on behalf of that group, but we believe that is a significant step forward to giving consumers better protection.

There are still certain things, which we might talk about later, that need to be done and there are still some challenges that need to be overcome. Notably, we need all banks to sign up to it, because it is a voluntary code. We need to resolve the problem of who pays, who reimburses the customer and how that customer is reimbursed when they are always not at fault. Then we need effective governance to make sure that we monitor the effectiveness of that code. The code will be judged on the success, and the success of all measures really should be judged on whether they result in fewer customers losing less money to APP fraud. That is what we all want to see. At the moment, if you look at the UK Finance figures, we are not seeing that, but the measures that we are putting in place should result in that.

Q530 **Mr Clarke:** Thank you both for being with us this morning. Mr Emery, what type of responses do you see from banks to people who suffer economic crime?

Richard Emery: They are dismissive, uncaring and obstructive. I am dealing with a case at the moment where the bank has said, "What has happened can only be explained by either option A or B. Option A means that we are at fault and option B means the customer is at fault. We know we are not at fault. Therefore, it must be the customer." Actually, from my experience of forensic investigation, there is at least an option C, which is that the bank is at fault, but it is just not willing to admit it.

I also have a particular frustration with banks that will not use the terminology. I have had an ongoing row with a bank that refuses to write to a customer and say, "We are not willing to refund the money because we consider that you have been grossly negligent." They do not want to put the words "gross negligence" in a letter to the customer because it will upset the customer. I am sorry, but that is the regulatory test. If that is the basis on which they are rejecting it, we want that in plain speak. I wrote back to the bank and said, "I want you to explain the way in which you consider that this person has been grossly negligent." In a nine-page answer, the words "gross negligence" appeared only once, and that was when they were quoting my letter.

Q531 **Mr Clarke:** Which banks are considered to be the best and which are the worst? Let us name and shame, because it is in the public interest. If banks are failing their customers, that needs to be exposed, and this is a platform on which to do it.

Richard Emery: Generally speaking, if you ask me, as somebody with a retail background, to rank a group of retailers, I would rank them from a positive scale through zero to a very small negative scale. If you ask me to do the same for banks, I would start at zero and go down.

Chair: None of them is great.

Richard Emery: As far as I am concerned, none of them is great. The two that I have the greatest concern about, and about which I have the greatest number of complaints, are Santander and Metro Bank.

Q532 **Mr Clarke:** Mr Piggin, Which? specialises in ranking the performance of companies large and small. Do you have the sense of any metric against which banks can be measured on this?

Richard Piggin: We do not have the figures. We do not have the data on which banks are more affected than others, or on which are the recipient or sending banks. We do not have that. I would say that this problem affects all banks. Part of the problem is a fundamental flaw in the payment system being used, which in the vast majority of cases is Faster Payments. Look at other payment methods that consumers use; the legislation acknowledges that there is a responsibility for those firms to use those payment systems. There is section 75 for credit card transactions. For unauthorised payments, it is in the PSRs. For debit card transactions, there is a voluntary agreement that enables customers to apply for a refund via the Chargeback rules.

There is no similar protection in place for Faster Payments. Yes, it affects all banks, but it is partly because we use Faster Payments and it is the Faster Payments system that is the fundamental problem here. We also need to look at what incentives we can put on Pay.UK, which now operates Faster Payments and other payment schemes, to improve those payment methods so that, regardless of whether it is Bank A or B, the system that they use has those inbuilt protections as well.

Q533 **Mr Clarke:** That is very helpful. Mr Emery, what is the percentage of cases that result in the victim receiving their money back, for both authorised and unauthorised payment fraud respectively?

Richard Emery: Can I deal with unauthorised first? I am sorry that I do not have a precise figure, because I am seeing the cases where the banks do not give the money back. I know, and I say to people, that banks do give enormous amounts of money back as a result of queries on unauthorised payment fraud. It is when they do not give it back that I get involved. I only see the problem cases, so it is very difficult.

In terms of authorised push payment fraud, my understanding and experience is that the banks only give back money that they have been able to recover from the receiving account. I might be a victim who has transferred £50,000 to a fraudster's account. By the time the banking system catches up, there is still £10,000 in that account. That money comes to me, but it is not the bank giving it back; it is the bank

recovering it. As Richard has said, it is often difficult for the banks to do that, because the speed of the Faster Payments system means that the money goes into the fraudster's account, tier one, and is then spread across several tier-two and tier-three accounts. You might identify some money down here. For me, one of the big issues is the fundamental regulatory basis by which the money left the tier-one account. I am the victim. My £20,000 goes into a tier-one fraud account. On what basis does the money leave that account? If that account has been opened in a fraudulent name, the bank has no authority to move the money out of that account.

Mr Clarke: Again that is a very helpful principle.

Richard Emery: It goes further than that. If we have an account that is opened with fake documents, and my £20,000 goes into that account, there is no owner of that account. There is no genuine account holder. On that basis, the banks have no right to take that £20,000 and move it on to the next level of fraud. The regulations say that, in the event of an unauthorised transaction, the bank has an obligation to restore the account to the state that it would have been in before the unauthorised transaction took place. If you apply that rule to that first-tier fraud account, the bank now has to put my £20,000 back into that first-tier fraud account. The only thing they can then do with that £20,000 is accept an indemnity from my bank and give it back, so we have a reverse route. The reverse route says that the money should never have left the tier-one account, and therefore it should still be there, and therefore my bank can claim it back. Where is the problem?

The problem is perfectly simple: I am the victim but I cannot make a complaint on the receiving bank. The only person who can make the complaint on the receiving bank and have the receiving bank account restored to that £20,000 is the genuine account holder, and there is not one. We have a fundamental failure in our current regulatory environment because we cannot work backwards. I cannot make a complaint to the receiving bank. I cannot make a complaint to the Financial Ombudsman service, because it is outside their jurisdiction. It is below the £100,000 threshold, so the police do not take any interest. If it is above the £100,000 threshold and we manage to get information about the receiving bank, we can get that information to the police, start court proceedings and the banks will say, "You cannot afford the costs."

Q534 **Mr Clarke:** That is helpful and it casts light on the regulatory implications. Mr Piggin, you alluded a little earlier to the contingent reimbursement model, and you were involved in its development. This sets out the circumstances in which the victims of APP scams will get their money back, and from whom. What do you believe it has the potential to accomplish?

Richard Piggin: I said before that its success will be judged on the impact it has on consumers and whether fewer consumers lose less money to APP fraud. What is clear is that this is a complex issue.

Richard has talked about various complexities. There is no single, simple solution, but we think some key things will happen. Firstly, we are encouraging all banks and PSPs to adopt this code, and it is a voluntary code. If we can get to that point, it will force banks to put in place some measures that they do not have in place at the moment. That will improve the experience for customers, because it should prevent more fraud. That is one good thing that we should get in place.

The second is that there is a principle agreed by those working on the APP Scams Steering Group, and shared by banks, that if the customer is not at fault—and, given the sophisticated nature of a lot of these scams, there are a lot of cases where customers could not have reasonably been expected to act any differently from you or I would have acted—they should get their money back. We are not in that situation now. If we get to the point where those consumers get their money back, it will be another significant step forward.

Q535 **Mr Clarke:** The CRM was originally meant to be introduced in September last year. We are now 14 months beyond the hoped-for implementation date. Is there a reason for that, other than the sheer complexity of the issue?

Richard Piggin: I am not sure that is correct. The PSR responded to our super-complaint in December 2016. It then spent a year without putting in place or proposing a contingent reimbursement model. It proposed that at the start of this year and then set up a steering group to help deliver it, and we were tasked with introducing a draft code for consultation in September this year that we hope, as a group, to publish early next year. There are challenges, and I have said this before: it is a complex issue and there are various and differing views on what needs to happen, as you would expect.

Q536 **Mr Clarke:** Has there been broad engagement from the banking sector? Realistically, are they going to sign up?

Richard Piggin: There is an equal split on the steering group between banking and consumer representatives, which is positive. The banking representatives on the group have been very clear. They have worked on the draft code. The consultation is now closed. They have worked on it and shown willingness. The proof will be in the pudding as to how quickly it can be introduced.

We will always say that we have been looking at this for years. Customers would expect banks to have already put some of these measures in place. Confirmation of payee is a case in point. When we launched our super-complaint, customers expected that, when a bank asks you to put in the name of who you are paying, the account number, the sort code and then a reference for you, so you can check what it is—maybe a holiday or a dinner—the bank would check that the account name matched the account number.

It transpires that banks are not and were not doing that, which is really odd from a customer perspective. They were told that the name they were putting in was simply a reference so that you would know who you were paying when you looked at your statement, but you were asked separately for a reference, so it was not clear to the customer that the bank was not checking those details. That is a fundamental measure that banks could introduce, but they have not introduced it.

Now you will see the PSR, as the regulator, consulting on a general direction to require banks to do this. Arguably, you could say that banks could have introduced this before, if they had wanted to, without necessarily being told that they had to introduce this measure. This is a measure that, although it will not prevent every bit of APP fraud, will stop quite a bit of it.

Q537 **Mr Clarke:** The Committee will be keeping a very close eye on whether they engage seriously with this when it is ready.

This is the final question from me, Mr Emery. I am conscious of time. We have already heard in this inquiry that banks should not be liable in all instances of APP fraud, because doing so would, "Attract more fraud into the system, not reduce fraud." Do you recognise that argument?

Richard Emery: I am sorry, but could you run that argument past me again?

Mr Clarke: That was somewhat my own reaction. None the less, for the sake of the record, "Were banks to be made liable in all instances of APP fraud, doing so would attract more fraud, not reduce it."

Richard Emery: The key word in there is "all". I fully accept that there will be occasions when APP fraud happens and, if you made banks liable all the time, you could get a network of fraud that is simply milking the system. There has to be a point at which you say, "Hang on. There is something much more serious going on here" and that the apparent victim is actually part of the whole fraud. For me, the liability has to go to the banks because the banks have the power and technical capability to put the systems in place.

I will just pick up something Richard said about confirmation of payee. I have a case of somebody who banks with Barclays. They created a payee in their system. It was, "I am going to make a payment to Simon Clarke," so the payee name was Simon Clarke. However, the account details were not yours, because of the way the fraud had developed. When this person keyed in to make a payment of £5,000 to Simon Clarke, he got back a text message saying, "Please confirm that you wish to make a payment to Simon Clarke", so the bank was playing back to him the name he had given on the account. Of course, he naturally believed that the bank was confirming that payee name with a beneficiary account, but it was not. It is that failure of confirmation of payee, and it should have existed for a long time. Having spoken to

Pay.UK, I believe that it will make a lot of difference when it comes in. It is one of the best things coming down the track.

Mr Clarke: That is a heartening note on which to end my questions. Thank you very much indeed.

Q538 **Chair:** Just before I hand over to Catherine, putting aside that this is an inquiry about economic crime and fraud, there will be instances where customers just make a mistake, particularly in the account number. Numbers get transposed. Do people come to you or do you have any experience of this? Are the banks good at this? The money is not being sent on to a fraudster's account, necessarily; it could be your or my account. A rogue amount of money appears. We identify that it is not something we were expecting. We might even tell our banks that this is a strange amount of money that has appeared. What is your experience of banks talking to each other to have that money sent back? If both customers realise there is a mistake, are the banks set up or even acting to help rectify those errors?

Richard Piggin: It is fat-fingered fraud. You type in the wrong digit and it goes to someone you were not expecting to pay. There is a process that the two banks will go through to dispute that transaction. Each bank will talk to their respective account holder. Where there is agreement, that money is just repatriated to the original account holder. It relies on the agreement of both parties, so the person who I have mistakenly paid, saying, "Yes, I was not expecting this transaction. I have never heard of Richard," that is fine. There might be occasions where the recipient says, "No, no, this is my money," and then a further investigation would need to happen.

Chair: Thank you. Fat-fingered fraud—we have learned another new phrase today.

Q539 **Catherine McKinnell:** That begs the question, if it possible to achieve an agreement. I am trying to get my head around this on behalf of constituents who have contacted me. I recently had a case of a disabled pensioner who got a phone call from someone who she believed was her television supplier, let us say—I am not going to name any names in this, because it is currently being investigated. She was subsequently contacted by someone who she believed was her bank, and it came up with the name of her bank on her telephone's caller ID. She was then told that the previous phone call from her television provider was not her television provider, and that had compromised her bank. They said, "We therefore need to rectify this, so we are going to create a new, clean and safe account for you. Would you please transfer your money to that without delay," so she did. Literally within minutes of putting the phone down, she thought, "Hang on. This does not stack up." She rang her bank. They said, "No, that was not us." She said, "It has literally just happened."

In the same way that between banks you could agree to refund money

where it is an authorised transaction but fraudulently so, apparently there is nothing the banks can do in that situation. People struggle to understand why, where they are legitimate transactions but mistaken—fat-fingered—you can organise for repatriation of those funds, whereas when knowingly between financial institutions there is a fraud, it cannot be done. Richard, you mentioned gross negligence, which brings me to my question. Is that gross negligence? To me, just because it was authorised, if you have no part at all in repatriating those funds, you have to have established gross negligence.

Richard Emery: When I start conversations with people who phone me in that situation, they say, "I have lost this money." My first question is: did you authorise it or did the fraudster take it? There are two avenues. The whole of the payment services regulations just deal with one avenue. They just deal with the unauthorised. The authorised goes nowhere. There is simply nowhere to go.

If I might, there were two words that you used that I picked up on, "without delay". There is a facility being written into the CRM that talks about vulnerable people being allowed to say to their bank, "We want Faster Payments to go slow. We want a situation where, when we authorise a payment, it does not go immediately." We need to understand the dynamics, as far as fraud is concerned. The vast majority of authorised push payment fraud and unauthorised fraud tied in with gross negligence happens within 24 hours of a key event.

The key event is the creation of a new payee. The fraudster cannot take money from my account unless they create themselves as a payee in my account. When a new payee is created, the clock starts ticking and the majority of high-value fraud, the majority of all that we are talking about, happens within 24 hours. Very interestingly, when I have conversations with banks about people who are claiming disputed transactions later than 24 hours, the banks say, "We are not convinced that that was fraud because it did not happen within the first 24 hours," so even the banks accept this. They have put it into CRM to allow vulnerable people to put in a delay.

I have to go on record and say that three years ago I wrote to the top 16 banks in the UK and said, "I want you to develop and implement 24-hour payment delay protection. From the moment I create a new payee, you are not to release any payment to that payee until after a clear 24 hours. In that time, please send me a text message, an email or phone me with an automated voice message, but tell me that I have created a payee." I also wanted the option for them to be able to notify a second party. If my elderly mother created a new payee, just the action of creating a new payee would result in me being told. I cannot stop the bank from doing it, but it would alert me that maybe mum is just making a mistake.

When I submitted that proposal for 24-hour payment delay protection to the banks three years ago, their response was entirely consistent: no. It

was no for two reasons. It was no because, "Our customers do not want it," but they have never asked. It was no because they argued that, from a regulatory perspective, they could not do it. That is not true now and it was not true then. What the Faster Payments scheme actually says is that the faster payment must be released within a period of time after it is authorised. If that authorisation says, "I'm going to be on holiday next week, so I want to set up a payment to go next Thursday," the faster payment clock only starts ticking next Thursday. If I said to the bank, as a matter of course, "Hold all high-value payments for 24 hours after the payee is created," they could do that. That is entirely within their regulatory and technical capability, and I hold all banks liable.

It is part of my whole campaigning about authorised push payment fraud. The people sitting behind me would not have lost the £450,000 that they have—just the people sitting behind me—if the banks had had 24-hour payment delay protection offered to their customers. It is a gross negligent failure.

I define gross negligence in a particular way. I wrote a paper on it that has now been published. I defined gross negligence as, "When an individual makes a conscious and voluntary decision to do or not to do something, with a clear understanding of a foreseeable risk of loss that is directly attributable to that action or inaction." The banks made a conscious and voluntary decision not to implement 24-hour delay protection and I believe that they had a clear understanding of the risk of loss that is directly associated with that. As such, the banks have failed for at least three years, apart from all the other failings we have already identified.

CRM is not going to be retrospective and it has to be or, as I have said and as Kevin Hollinrake has said, there needs to be an alternative scheme created to allow past and present victims of push payment fraud to recover their money. The very fact that it was meant to be implemented in September and will now not be implemented until January means that a whole bunch of people would have been covered and are not. That has to change. There has to be a scheme in place that brings the banks to account. The headline figure—this is my estimate—is that something like £1 billion should be refunded to customers who have been the victims of push payment fraud between 2014 and 2018.

Q540 **Catherine McKinnell:** Just for clarity, are you saying that that should apply to a self-designated vulnerable customer or to everybody?

Richard Emery: I am saying that 24-hour payment delay protection should be something that all customers can opt into, but I would suggest that you have to opt into it.

Q541 **Catherine McKinnell:** The difficulty with this type of crime is that you do not think you are vulnerable to it until it happens to you. People who are victims of this crime would not necessarily define themselves as vulnerable.

Richard Emery: That is correct. There is a debate as to whether the default should be that banks turn it on.

Catherine McKinnell: You should opt in if you want Faster Payments.

Richard Emery: You have to say you do not want it.

Catherine McKinnell: Yes, "Because I am invincible."

Richard Emery: It is important that it is in place all the time. One bank has responded by saying, "We are implementing a system now that allows people who are suspicious about a payment that they are going to make to defer the payment for 24 hours." I do not think they quite understand the situation. That is not the time to make the decision. You have to make the decision up front. I have asked a lot of people, "When was the last time you made a payment of more than £500 to a new payee, when you did not know the payment details 24 hours in advance?" I have only ever had one person with a positive reason where it would be a problem.

Chair: Or they have had to wait 24 hours.

Richard Emery: Everybody else can wait 24 hours. If you are paying money to your solicitor for a property purchase, you know their account details in advance. If you are paying a supplier, you have the invoice. You have it in advance. My own policy, if I am paying a large sum, is to create the payee and then send them 79p. Then I will phone them up and say, "Have you got my 79p?" "Yes." "Fine, now I know I can pay you."

Q542 **Catherine McKinnell:** That is what some payment systems do in order to create the transaction; they put in £1 and then take it back.

Looking at gross negligence again—not necessarily your definition of it, but the use of gross negligence as a reason by the banks not to refund customers—do you think it is used consistently? Do you think it is well understood? Does more need to be done to define it and make sure it is used correctly?

Richard Emery: As of 22 August, when the Financial Ombudsman service published its quarterly newsletter and said the bar is now higher, I am hopeful, but I am only hopeful at the moment because I am waiting to see how it works out. I am still in the situation where—and I will name them—Metro Bank writes out letters to its customers and does not refer to the customer being grossly negligent. At the moment, Metro Bank has certainly not accepted the new approach to gross negligence. Santander has accepted it. We are hoping to gradually work through a number of cases with Santander. With other banks, I am hoping. Of the two banks I have had the biggest issue with on gross negligence, Santander appears to be accepting the new approach and Metro Bank appears to be fighting it.

Q543 **Catherine McKinnell:** Are we seeing examples of banks citing lack of due care as a reason not to refund?

Richard Emery: I would go back to them and say, "That is fine; I do not care about due care." I could tell you some quite funny stories of when banks have said that the customer has been negligent, and I have written to the bank and said, "Thank you very much. If the customer has been negligent, refund them, because they have not been grossly negligent." The bank has written back and said, "We have reviewed the case. The customer was grossly negligent."

Catherine McKinnell: A lot of customers do not have the benefit of your support in this situation. They are dealing with the banks directly.

Richard Emery: That is why a year ago, when I realised this was an issue, I went to the Financial Ombudsman service, because I knew the place where this had to change was with the Financial Ombudsman service. Once it starts ruling against the banks, the banks will have to take notice.

Q544 **Catherine McKinnell:** Just moving on to the broader landscape and criminality of these frauds, do you find that people go to the police and report these crimes or do they tend to try to deal with them through the bank and, failing that, give up? Do you think the police have enough capacity to deal with these crimes?

Richard Piggin: I am happy to talk to this. We hear from customers and consumers in terms of their experience of reporting fraud and, on the whole, it is highly unsatisfactory. There is still some confusion over who you should report it to. Should you report it to your bank, your local police force or to Action Fraud? The general advice is that you should report it to Action Fraud, but in the cases that we have talked about of online transfer, actually, you need to report it to your bank first, because speed is of the essence and the bank is the best place to intervene in the first case.

You report it to Action Fraud, but Action Fraud does not have investigative powers. They collate that, which is useful to get a sense of the general trends of fraud. They might pass it on to the NFIB, which might pass it back to a local police force, if there is a case for it to be investigated. Now, this takes time. It often comes back to the local police force and you will get a letter to say, "There is no viable lead of inquiry, so your case is closed." In general, it is a very unsatisfactory experience.

Which? did an investigation that we published in October. We sent freedom of information requests to local police forces and two-thirds of them responded. We found that their success at investigating fraud had dropped by, for the majority, over 20% between 2014 and 2016. We estimate that less than 4% of online fraud is successfully investigated by the police. I can send you the full article.

Q545 **Catherine McKinnell:** Do we have a full picture? If a victim went to the bank rather than to the police, does the bank have an obligation to notify Action Fraud of the levels of fraud? Do we have a complete picture of the levels of fraud?

Richard Piggin: I do not think we have a complete picture. To add to that, there are a lot of cases that go unreported for various reasons.

Q546 **Catherine McKinnell:** Would it be helpful to encourage more reporting, or to encourage or require banks to report fraud to Action Fraud?

Richard Piggin: You need a joined-up approach, yes, to encourage more people to report, but then you need some sort of co-ordination between police, banks and Action Fraud. Almost three years ago the Government set up a joint fraud taskforce. It is unclear, three years later, what that taskforce has done, what impact it has had, the transparency of its workstream and the progress it has made. That is fairly unacceptable. The co-ordination and that joined-up approach are needed.

You mentioned a scam earlier that involved a fraudster spoofing the number of the bank. Fraudsters will do this. That involves the telecoms companies and Ofcom, which are probably better placed to address that particular flaw in the system. They need to work together with the banks, and perhaps with the regulator, to implement a solution. That is something that perhaps the joint fraud taskforce could focus on, but it is not clear what work it is doing and whether that joined-up approach is actually happening.

Q547 **Catherine McKinnell:** You have identified examples of significant levels of money being extracted through these fraudulent scams, but there is a huge amount of serious but low-level fraud, small transactions that the banks are refunding and obviously not then reporting as fraud. Is it the case that, while these small amounts of fraud are going on, I would suspect on a vast scale, and not being reported, we are not getting the big picture? Are we creating an environment in which small-level fraud then increases to large-level fraud, and therefore, just from the figures that you stated about the amount of fraud that is being dealt with and recovered, we are losing the battle here, unless we take some serious action to get both the full picture and put in adequate resource to get on top of the scams that a lot of people are faced with?

Richard Piggin: There are huge challenges in acting after the fact. Once the fraud has happened, there are huge challenges that the police and banks face in resolving the issue and putting the customer back in the position they were in before. That is why the focus should be on preventing the fraud from happening in the first place.

Richard Emery: While I agree that this is the way we are going in the future, if we look back at the past, some serious issues have gone on. Fundamentally, the police do not have the resources to address this issue properly. We are in a situation where, broadly speaking, if a report to Action Fraud is for less than £100,000, it will not be investigated. You

have that threshold. People come to me and say, "I have reported it to Action Fraud. What do I expect to happen next?" My response, if it is less than £100,000, is "Nothing."

This is where I would like to share with you network-level transactional data analysis. We understand the banks have reported 80,000 cases of authorised push payment fraud in 2017 and the first half of 2018. A lot of those are going to be very low value.

Q548 **Chair:** The £100,000 is not just one case. Do they have the information to look at the cumulative impact of a number of cases, which are clearly going to the same people, the same accounts or the same places around the world?

Richard Emery: That is what network-level transactional data analysis is. I want UK Finance to disclose to a working group the details for the 80,000—"This is where the money started and this is where it went." We can then profile how much there is in terms of how many low-value crimes, low-value consumer scams, high-value consumer scams and expected payment frauds. We can work out the scale of the different values. That will help us to understand.

Most importantly, network-level transactional data analysis on the last 18 months of data will give us three very important pieces of information. It will identify the banks that have received most of the money. They are the people hosting most of the accounts used by fraud. It will allow us to identify the branches within those banks. You may or may not be aware of a recent case of a branch manager for one bank who was found guilty of being party to a fraud. He opened 400 fraudulent bank accounts and sold them to fraudsters who processed £16 million through those 400 accounts. That is what ongoing network-level transactional data analysis should pick up, but I want to do it historically and look at the past.

It will also identify, as you have just said, those accounts that have received large amounts of money, but that are the composite result of lots of individual frauds. If we ran that network-level transactional data analysis for the last 18 months, we would have something we could take to the police and say, "Here are the top 10% accounts by value. Now, banks, you have to give that money back." That is the whole process. UK Finance has said that the biggest problem with receiving accounts is money mule accounts held by students between the ages of 16 and 25. I have not seen any statistical data to validate that statement. When the retail fraud director of Lloyds went on record, he said he could identify a student account that had operated normally but was then used for money muling. Some £100,000 went through that account in a short space of time, but the bank did not notice it, because it does not have effective monitoring.

Q549 **Chair:** I agree. I can tell you, representing a university town, that I do not know of many students who would have that much money flooding through their bank accounts. To the point you made about telecoms

companies, in the TSB cases, many involved SIM cards being fraudulently obtained from a particular provider. I think it was EE. That assisted in terms of the telephone calls that then triggered the fraudulent activity. What people reported to us would ring true with your experiences.

Richard Piggin: Yes, there are other players in the fraud ecosystem that have enabled aspects of fraud. The commonality is that the frauds happen because money has been transferred from one account to another. That is common across the board but, in cases where there are other aspects, those entities should take more responsibility because they are best placed to put in place measures that will prevent that type of fraud.

Q550 **Chair:** Apart from telecoms companies or mobile phone operators, would you point your finger at anybody else in particular?

Richard Piggin: There are particular online platforms, such as holiday letting platforms, where we have seen an increase in the amount of fraud. They put in place certain protections, that you should only pay through those sites, but perhaps there is more that they could be doing to take down fake listings. Which? did an interesting investigation into how easy it was to place fake listings on some of these sites, how quickly they are removed, what action is taken and how they are reported. That is one particular sector. Then perhaps, given the impact of invoice or mandate fraud, you could look at the role of solicitors or internet service providers when emails are hacked. Is there a vulnerability in their systems that they could improve that banks have no ability to make better, but the internet service providers, the email providers or maybe the firms that have had their emails hacked could do more?

Q551 **Chair:** What about dating sites?

Richard Piggin: Given the scale of romance scams, there is perhaps more that they could be doing as well.

Chair: One constituent got particularly caught up in that.

Q552 **Colin Clark:** Moving on from romance, Mr Piggin, you have brought me neatly to my subject. I want to speak about educating consumers in fraud prevention. However, in all the evidence I have listened to, I worry there is obfuscation by the banks and others responsible to try to say, "We need to improve consumer education and it will all go away." Mr Piggin, you made the point that you want to prevent the fraud rather than deal with it after, so I will carry on with my planned route. What resources are available to consumers to educate themselves about risks around scams, considering how sophisticated they are?

Richard Piggin: Considering how sophisticated they are is the key point and the fact that, by their nature, these scams constantly change, evolve and become more sophisticated.

Colin Clark: The scammers will constantly stay ahead.

Richard Piggin: Absolutely. Looking at an education or awareness-raising campaign, those messages must constantly evolve and be re-delivered to the customer, which is a challenge. It then relies on the customer receiving those messages, and not all customers will receive those messages. It then relies on the customer reading and understanding those messages. Finally, it relies on them remembering what to do at the point at which they are being scammed. All of those are very high thresholds for success. While there is definitely a role for education, and I have mentioned before that *Which?* magazine publishes articles and offers insight, tips and advice to consumers. That is very important, but it cannot be the only thing and it cannot be the thing that we rely on. Too much responsibility is placed on consumers to protect themselves from sophisticated scams.

Richard Emery: I entirely agree with that. The issue is the point of vulnerability. Mr Clark, you are a doctor sitting in your surgery. Your jacket is on your chair. Your receptionist phones you up and says, "We have an urgent phone call from the bank. Somebody in the bank is trying to withdraw £4,500. They have your debit card." "My wallet is gone. Put them through". "Hi, this is ABC Bank. We have somebody in front of us at the moment. We need you to give us your four-digit code, so that we can block your card." It is that point of vulnerability. What is more is they proved who they were because, when the bank phoned through, they said, "We are from your bank. We can confirm we are from your bank because yesterday you spent £37.48 on petrol at the local Esso station." How did they know? The receipt was in the wallet that was stolen.

Q553 **Colin Clark:** I can see that a lot of my questions are going to lead to some fairly obvious answers. To go back to the beginning—and I am slightly sceptical about this—you have mentioned students a number of times. Are the students involved in the fraud or are the accounts false?

Richard Emery: UK Finance will say—and I agree—that there are literally hundreds, potentially thousands, of students who are allowing their accounts to be used to process stolen money.

Q554 **Colin Clark:** How does that work? They cannot be told it is fraud, because I assume that they hopefully would not do it. Are they just making money?

Richard Emery: No, they are offered a job to receive payments from overseas companies and then pay them into the relevant UK account, and they get 10%. The figures that I have seen are only a tiny microcosm of the figures, but I have seen two figures. One is a figure from Cifas that says they have identified 8,000 money mule accounts. There is a figure in the public domain because it was spoken of on Radio 4's "Money Box", by the retail fraud director of Lloyds, who referred to the fact that they had done a trawl of their systems and found 13,000 accounts being used for money muling, the overwhelming majority of which were in the age

range 16 to 25. That is where the problem exists. Those students are committing a criminal offense. There have been 200 prosecutions.

You need to start getting those people in who have allowed their accounts to be used, and put police resource in so that you can bring in these people, interview them and give them a criminal caution. Then, have a public campaign that says, "2,000 students across the piece have all been given criminal cautions," which means they now cannot open bank accounts, take out phone contracts or travel to America without special consent. Until you start attacking them, the police will say that they are interested in getting the money mule masters. I agree with that, but if you put some resource in at the bottom level and make the students aware that this is criminality, they will be punished and they will suffer a very serious consequence. That has to happen. I agree that there is a problem with money muling, but it is not being properly addressed.

Q555 **Colin Clark:** Mr Piggin, can I take you down a slightly different route? You already mentioned social media in your evidence. As we have heard about authorised push payment fraud, people can give away their passwords, their bank cards or even actual cash to fraudsters. What part is social media contributing to it? Is it creating a vulnerability?

Richard Piggin: There has been a rise in social media scams, WhatsApp scams and Facebook scams. I mentioned holiday booking before. Technology has made it perfectly normal to book a villa and pay a stranger for a villa or an apartment on holiday, without ever meeting that person or seeing that villa or apartment, apart from on the internet. That is normal behaviour. When you see it on a Facebook site, on WhatsApp or through social media, you are encouraged to pay via bank transfer. The fraudsters are utilising social media to reach potential victims. That is what we are seeing and why I talked about the rise of social media scams.

Q556 **Colin Clark:** If we can move on a little, banks have recently undertaken prominent advertising campaigns. This comes back to my original point that I am worried about obfuscation of what they are trying to do. How effective have the campaigns been? Without leading the witnesses, are they trying to cover themselves or genuinely trying to move this forward?

Richard Piggin: I said it before: there is an important role for education and awareness raising, but the response from banks so far has been to focus on that measure. You will see lots of campaigns from banks. Some of them are pretty good and they have a real place because they will reach customers and make them think. Despite some of these adverts highlighting how sophisticated the fraudsters are—so the banks are acknowledging how sophisticated this fraud can be—there is little evidence yet that shows what impact those campaigns have had to reduce the amount of fraud that is taking place.

Richard Emery: I agree entirely with what Richard has just said.

Q557 **Colin Clark:** Thinking about that and what has been going on recently, is the reduction in branches and face-to-face banking making consumers more vulnerable? Is it modern banking? You have spoken about Faster Payments, which I use all the time, and you have terrified me. I could give you an example of having to pay somebody quickly, whose details I did not have—it was IPSA's fault, but I will not go into that. Is it modern banking and that lack of face-to-face interaction? I suppose I am being stereotypical in saying it is making older people more vulnerable, but is that disconnect making everybody more vulnerable, because we think we are doing things so much faster and more efficiently, and we think we are protected?

Richard Emery: Speed is one issue. The absence of face-to-face means that we are much more used to the idea of either us phoning the bank or the bank phoning us. That telephone contact makes us more vulnerable. I think this is going to be true of just about every bank, but it is certainly true of the two banks I am most concerned about. If you want to go online to your Metro Bank account, you have to put in your 12-digit code and then selected digits from a secret number and a secret word. If you are phoned by Metro Bank, they will ask you for your 12-digit number and selected digits from the same secret number and secret word. You have one secret number and one secret word, and they gain access either through the online or through the telephone system.

You receive a text message that says, "We are concerned about this particular transaction. Please phone this number." You phone the number in the text message and the person says, "Metro Bank, what is your 12-digit number?" They are keying it into the computer. Then the computer is asking them what digits the fraudster needs to access your bank account, so they ask you, "What are the second and third digits of your code? What are the third and fourth digits of your password?" You are answering those questions because you believe you are talking to Metro Bank, because that is the process.

One of the things I would say, which I know may sound daft at first hearing, is that I believe that all banks should remove all contact telephone numbers from all text messages. You should receive a message that says, "This is a message from NatWest bank. Please phone us from the number on the back of your card." If you did that across the whole piece, if all the banks did that consistently, then there is an education message that says, "We will never ever give you a phone number in a text message." That means that when people see a phone number they will go, "Hang on. That should not be there." What actually happens is the phone number in the text message is an instant connect. You see the message, you press the button and you are connected. You are talking to a fraudster. There are areas like that, which I hope gives you more of an insight. That is the way they get in.

The other way that they get in—and I have a couple of cases like this at the moment—is where the fraudster already knew the 12-digit number,

the whole of the security number, and the whole of the password because, at the time they phoned the victim, they were already in the account. When they spoke to the victim, their first point was, "I am phoning you from Metro Bank because somebody has tried to duplicate the £5,000 payment you did three days ago." That is because they are already in the account and we now have evidence that that is the case. The question is how the fraudster got not just selected digits from your code, but the whole code. As far as I am concerned, that must indicate that there is an issue within the banking system rather than with the consumer. Consumers do not go around saying, "I just want to tell you my eight-digit security code and secret word for my bank account." Consumers do not share that information. In my opinion, if that information is in the hands of the fraudster, it has come from the bank.

Q558 **Colin Clark:** The banks have pushed modern banking and said that consumers demanded it, but did consumers sign up for more vulnerable banking to get more modern banking? One of my other questions is about the technical solutions. You have just given a technical solution, Mr Emery, of saying to dial the number on the back of your card, not the number they are sending through. Is there not a moral and legal responsibility on the part of the banks? They have moved us to modern banking, which has left us fundamentally more vulnerable than we were before?

Richard Emery: Yes.

Q559 **Colin Clark:** Mr Piggin, do you agree that consumers had an option? Has this been driven by consumers? You have mentioned Metro Bank and banks that do not have many high street branches. Have we been led down a path? Considering Which? asks consumers all the time, is this where we wanted to be, but we did not realise that the result would be that we are more vulnerable?

Richard Piggin: There are clearly lots of benefits to online and mobile banking, and consumers value those benefits. They like being able to check their account and make payments instantly from their phone. They like being able to log on. A proportion of consumers have absolutely demanded that, because some banks have offered it and they are very popular banks. There is a question, when we talk about branch closures and face-to-face banking, about whether it is demand-driven or not. If it is and that is in response to the way in which consumers are behaving, that is one thing. If it is forcing consumers to behave in a different way, that is another.

Your point about ensuring that the systems that the banks have in place to protect their consumers are adequate is completely valid because, if consumers are using online banking, internet banking and mobile banking, there is an expectation that it is safe. There is an expectation when they use these services that they are safe, and it is the responsibility of the banks and the payment systems involved to ensure that they are safe. If there are flaws in security and account opening

processes, they need to be resolved. That is clear. If there are also flaws in the technology, they should be addressed.

I get text messages from my bank all the time, and it appears as though they come from the bank. If I look at the number, the short code comes from the name of the bank. It is easy to spoof that and send me a message that is not from my bank, but appears as though it is. It will appear in the same thread as other genuine messages, so how, as a customer, would I know whether the message that I have received from my bank is genuine? There is therefore an interesting question: if banks know that there are vulnerabilities in communicating via text messages, why do they communicate with their customers via text message? If there are flaws with their security systems when they are asking for passcodes and personal details as part of their security when they call you and speak to you on the phone, which they know can be imitated successfully by scammers, is there not an obligation on them to improve those security measures consistently and constantly to fool the scammers and so the scammers cannot use them?

Q560 **Colin Clark:** You were speaking about trying to warn people about scams. If you then start warning people by email and text about scams—this gets worse—you are potentially setting up a scam. One of my questions is what more we can do technically. I am sounding terribly old, but you could move back to some sort of traditional relationship with somebody who you know at the end of the phone, but that, of course, is no longer most people's experience of banking.

Richard Piggin: Sometimes it is just not feasible or practical to have that, and again customers do not want it. If they want to make a transaction, they might not necessarily want to find a date in the diary when they can go into a bank and make that transaction. There is some give and take here.

Richard Emery: When you have a bank that has historically allowed online payments of truly eye-watering proportions to be made without identifying that something might be going wrong, if anything, that gets me really annoyed. I am going to say this. There are two people sitting behind me. Alex lost £180,000 as a result of 30 £6,000 transactions going out of her account, an account that, in the previous six months, had never had more than £6,000 go through it in a month. There were new payees created due to a flaw in Santander's security system. They created 16 new payees. When I eventually raised the issue with Santander at the beginning of April last year, it amended its security protocol but has never been willing to refund the money. Alex is just one of a number of people who lost significant amounts of money.

We have a gentleman sitting here who is a friend of Lisa. Lisa received a phone call that she genuinely believed was from her bank. At the time she received that phone call, she had £0.25 million in one account and modest amounts of money in two other accounts. The fraudsters persuaded her that she had to engage in an account transfer. She

created the new payee and made a payment of £20,000, because that was the maximum amount the bank allowed to be paid in one go, but the bank allowed multiple payments of £20,000. The bank did not notice when she made a second, third, fourth and fifth payment—£100,000. The bank did not then notice when she transferred the remaining £150,000 out of that account, because she had hit the account limit, into another account and did five more payments of £20,000, totalling £200,000. She then transferred the rest of that money into the third account and did four more transactions, £277,000, and the bank did not notice.

The only thing that I can say about Santander is that, as of the last few weeks, they have at long last fundamentally changed their online payment system. I talked to them only yesterday and said, "Can you please confirm what your transactional limits are?" They said that they are now entirely account-dependent and based on the account history. If you want to make a large-value payment, you have to phone them. They will take the details and then phone you back on your registered phone number. Santander was written to by this lady's MP in the middle of August and took six weeks to reply. It was written to again and has not replied six weeks later, but it has actually now appeared to act.

I sincerely hope it goes back to Lisa's account, to Holly's account and to the accounts of others who have been the victims of their failed systems. This is a case of where push payment fraud is actually the responsibility of the sending bank, because it has allowed their customer to send the money. It is a disgrace and it has changed. I hope they have put it right now.

Q561 **Chair:** I strongly suspect that Santander's government affairs people will be carefully scrutinising this session and will have heard all your evidence very clearly. I have a couple of final questions. I mentioned earlier our inquiry into vulnerable customers' access to financial services. We have also just launched an inquiry into online resilience, for the reasons you have set out, Mr Piggin, which are how important it is these days for people using online and mobile banking systems that they are as resilient as they need to be to cope with demand and problems.

When we talk about vulnerable customers, the definition is very broad. Obviously there are some people who might always be considered to be vulnerable. There might be others who are vulnerable at a particular stage, because of life events. You mentioned powers of attorney and acting on behalf of other people. Mr Emery, earlier you mentioned a case you are dealing with of a gentleman with a brain injury. We have also had evidence in that inquiry from a lady who was blind who, in order to pay a taxi driver, had to give him her PIN. He was trustworthy and did not do anything he should not have done, but that was an immediate vulnerability where she has handed over a critical piece of information and could later be subject to criticism, if something had gone wrong.

Earlier we explored the socioeconomic background of the complainants

you see, and I wondered whether there is anything you want to say about vulnerable customers. In the casework you have, are there people with particular vulnerabilities? Mr Emery, do you think this is a particular area where the banks could do even more than you have already said they should be doing for all customers?

Richard Emery: Banks should allow people—if I could pick up the terminology you used—power of attorney. The situation for the banks at the moment is that either you have control of your account or you have power of attorney. They currently do not have provision for what I call "second-party notification." I do not want to be able to control my mother's bank account and I do not want responsibility, but I want to know what is happening. For me, that is a soft way of beginning to help. People do not necessarily want to admit that they are vulnerable, but if I turned to her and said, "Look, Mum, it would just help give me confidence that, if ever anything did happen, if ever you were the victim of a scam and somebody was trying to make you make a high-value payment that you did not mean to make, can you tell the bank that they can tell me about certain things?" For me, second-party notification would be a big step forward.

Q562 **Chair:** Mr Piggin, is there anything from Which?'s experience in the complaints that you have been handling?

Richard Piggin: I have nothing more to add to what you said before, apart from saying that the reimbursement code makes specific consideration, not for vulnerable consumers as such, but for consumers who are vulnerable to APP scams. It treats them differently for reimbursement, which would be considered on a case-by-case basis, which is appropriate in my view.

Q563 **Chair:** On the messages we have talked about and education, do you think there is more that the banks could be doing to work with customers with particular vulnerabilities, over and above, to remind people, perhaps people who have caring responsibilities, about opportunities for fraud?

Richard Emery: The caring issue is why I am putting forward the idea of second-party notification. It ties in with the carer aspect.

Richard Piggin: Generic awareness-raising campaigns are challenging in terms of their impact. We would welcome more specific targeted information given to customers based on their circumstance, and we would want to see banks do more to develop that. If you are in a certain situation, that bank recognises that situation and gives you warnings that are effective because they are tailored to your particular situation, rather than a generic warning of what to look out for.

Chair: We are very grateful to you for your evidence. Is there anything else? You have been very generous and given us lots of your expertise and thoughts. Is there any other burning issue you came with that you wanted to draw attention to today that we have not covered?

Unfortunately, I cannot take evidence from the public gallery. I would just say thank you to our witnesses. Thank you to those who have sat through the evidence session. I know that there are people in the public gallery who have been particularly affected by the issues that we have explored today. We are grateful that, through Mr Emery, you have been able to share some of that experience.

Our inquiry is open to anybody to submit written evidence. It does not have to be long or complicated. We cannot, as a Committee, look into individual cases, but anything that people tells us helps to build up a picture for our report. We are able to put it in the report but also quiz other witnesses, including trade bodies, banks and financial institutions about it as well. If there are further issues or stories that you want to raise with us or make us aware of, we would be grateful to those bringing them in. I am sorry to the gentleman in the public gallery, but perhaps we can have a chat or a quick word afterwards. Thank you for your time this morning.