HOUSE OF LORDS

Fraud Act 2006 and Digital Fraud Committee

Uncorrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 10 March 2022

9.25 am

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Lord Allan of Hallam; Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Lord Gilbert of Panteg; Baroness Henig; Baroness Kingsmill; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 4 Heard in Public Questions 34 - 43

Witnesses

I: Geraldine Lawlor, Global Head of Financial Crime, KPMG LLP; Brian Dilley, Group Director, Fraud and Financial Crime Prevention, Lloyds Banking Group; Nicholas Taylor, Head of Policy and Public Affairs, Revolut UK.

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.

3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witnesses

Geraldine Lawlor, Brian Dilley and Nicholas Taylor.

The Chair: Good morning and welcome to this evidence session of the Fraud Act 2006 and Digital Fraud Committee. A transcript of the meeting will be taken and published on the committee website, and you will have the opportunity to make corrections to it where necessary. We are delighted this morning to be joined by Brian Dilley, the group director of economic crime prevention at Lloyds Banking Group, Geraldine Lawlor, global head of financial crime at KPMG, and Nicholas Taylor, head of policy and public affairs at Revolut. Thank you, all three, for being here. Without further ado, I will ask Lord Young to put the first question to the panel.

Q34 **Lord Young of Cookham:** Good morning. Can we start with authorised push payments, which the Joint Fraud Taskforce has identified as the major problem for financial institutions?

It is a three-part question. First, what are the financial institutions doing to disrupt and restrict the fraudsters who are operating the system? Secondly, what are they now doing to try to get round the measures that you are introducing? Thirdly, is there anything more that the Government should be doing in order to assist the efforts that you are making?

Geraldine Lawlor: I suppose the question is really aimed at the banking sector and the initiatives it is running in this particular area. A lot of work has gone into the authorised push payment schemes by the industry through prevention strategies, such as raising education and awareness, improved technology, working on mules, sharing intelligence across the banking sector, and the typologies of particular frauds and scams, to make sure that consumers are aware of the vulnerabilities they face, and looking at prevention in that area, as well as looking at capabilities and technology to detect when scams have been identified and how they are disrupted.

The industry has put a lot of customer authentication controls into the system to try to validate who they are dealing with and to support consumers in that endeavour, as well as putting controls at the point of transaction to raise awareness to the individual consumer and ensuring that it is not a fraud, asking them to stop, check and challenge before they press the button to transact.

Perhaps I should hand over to Brian or Nicholas, who have more insight from the front line of what they are doing in their respective institutions. This is an area that is evolving all the while, and they will probably have the most up-to-date position.

Lord Young of Cookham: Brian, are you winning?

Brian Dilley: It is a never-ending battle. In terms of the difference between authorised push payments and traditional unauthorised fraud, the biggest challenge for us is our customer processing the transaction.

Often, they have been coached by the fraudster to give a story to the bank, and they often lie to us because they think they have been told by the fraudster that they should tell that story. Often, they say, "The bank is in on it, so you don't want to tell them the truth".

What are we doing? We have a multi-layered set of defences. We use analytics over the transactions to identify those that are most likely to be scams and stop them and ask additional questions. A lot of the authorised push payment defences are around the behaviour of the customer. We have analytical tools that we use to look at the way the customer is behaving and the way the customer is interacting with us, to look for signs that they might be under duress and that they might be doing something different from what they normally do. That is another indicator that they might be being scammed.

We have a series of warnings; we reach out to the customer and so on. We have worked with behavioural psychologists to see where in the journey the customer is most likely to respond to a warning, and how that warning should be phrased to try to take them out of what is often called the hot state that they are in when they believe the fraudster, and always believe that their money is at risk and they need to act urgently; when they are not thinking straight and act urgently. Then we have a number of things like the banking protocol in branches; we have an arrangement with the police whereby we can call them if we suspect that the transaction is a scam. We have all those defences.

How are the fraudsters evading us? The one big thing is that, as we put anything in, they see it very quickly and adapt. One of the big areas is where the proceeds go once we put in confirmation of payee. A lot of the payments were diverted to banks that do not have confirmation of payee. That is a good example of the adaptation of the fraudsters.

As regards what we need from government, first, we are really pleased to see the change in the online safety Bill and paid-for advertising coming under that. That works really well. The other part is that the whole ecosystem needs to be involved in the defences, not just the people handling the transactions. The telecoms and the online firms must all work together to try to reduce this, with some system leadership to try to get it all working together as a wider ecosystem.

Lord Young of Cookham: You talked about the dialogue you have with the customer you think has been defrauded. What percentage of customers do you convince that it is a fraud and that the payments should stop? To what extent does the customer just go on? Are you able to put any sort of figure on how effective those interventions are?

Brian Dilley: It varies in different channels and in different types of scam. In branches, it is quite helpful that you have the person in front of you. If they are talking to us on the telephone, again, you have an interaction. If it is an online payment and we are reaching out to them, sometimes the challenge is getting the person to respond. One of the challenges is the person believing that the person trying to contact them

is genuinely trying to help them and is from the bank, because that is part of the narrative that the fraudsters use. They call you and say, "I'm from the fraud department at the bank and I'm trying to help you, and you now need to move all your money". I do not have a detailed breakdown of the individual types. The statistic I have is that across the banking industry we prevent two-thirds of the fraud that is attempted. In effectiveness, that is a pretty good hit rate, but one-third is still a very large amount of money.

Lord Young of Cookham: Nicholas, do you want to add a footnote to what your two colleagues have said?

Nicholas Taylor: Yes. I have the statistic for you. Our machine learning models correctly identify over 90% of attempted APP fraud, but of customers we then warn—that 90%—85% ignore the warnings, and that is after direct human intervention. It is incredibly difficult to break the spell. We have all the normal warnings before you make a transfer, but our models detect and block a payment post fact, where we think it is a fraud, and then we make the customer talk to one of our agents. Even after we have directly intervened, 80% of them still go on to make the payment.

Lord Young of Cookham: That is a very worrying figure. How do you identify the 90% of fraudulent payments? Do you have software?

Nicholas Taylor: We have very advanced machine learning models that have 200 or 300 different data points feeding into them. They have been built in conjunction with former law enforcement officials, former financial institutions and some of the best data scientists and engineers that we have at the company. We treat financial crime and APP fraud like any other product. We put some of the best minds in the technology business on to it and combine that with law enforcement expertise. These things improve constantly. It is machine learning. We feed in every fraud we miss, and the model learns and gets better.

Lord Young of Cookham: Is the software that you are using shared with other institutions, or is it specific to you?

Nicholas Taylor: We share best practice and the types of fraud we spot, but each institution has its own models. They use common frameworks, but you cannot pick ours up and put it into a Lloyds or another bank. We are always looking for ways to learn from each other as institutions.

Lord Young of Cookham: Thank you very much. That is a really helpful start to our session.

Q35 **Lord Browne of Ladyton:** Good morning, everyone, and thank you to our witnesses for coming. Staying on the issue of prevention, can we turn our attention for a few minutes to what financial services businesses do to educate their customers about fraud, increase awareness and draw their attention to tools or behaviour on their part that can help protect them against it? The questions are pretty basic, but they are intended to drill down.

What do you actually do with your customers? What is your assessment of the success of these programmes? Brian, could you talk us through the key campaigns that you have to raise awareness, and then maybe we could move on to an assessment of how successful you think they are and how we could help to improve them?

Brian Dilley: Sure. There are those that we do as Lloyds and there are those that we do as the industry. As Lloyds, a lot of it is linked to the things that I said about behavioural analytics and warnings. We have educational material that we ask customers to look at and require them to view at certain points. Under the banking protocol, if we suspect a fraud, there would be an in-branch discussion of the types of fraud we see—in-the-moment education, if you like. We have wider warnings and data that we regularly share with customers.

The main educational piece for the industry is the Take Five campaign, which has been running for several years. It is run by UK Finance, and the banks contribute funding. The latest data from that is that a quarter of the public record the current campaign, which is Stop, Challenge, Protect, and that two out of five recognise the Take Five banner, which we have on all our ATMs and all our apps, and in all the different banks. That is good. Obviously, we want recognition and awareness of it to be better.

We have had a partnership with the City of London Police for three years, going into its fourth year now. We have developed a school training programme called Cyber Detectives, where we go into primary schools and teach children. We are not going in and preaching fraud; we teach them about dishonesty, and detecting dishonesty. We teach them about safety online and things like that. It has a lot of messages, on one side, on how to spot that someone is trying to scam you in everyday life as well as in banking, and, on the other side, the challenges of being a money mule, because schoolchildren are targeted for that. That has been downloaded by over 3,500 schools and is PSHE-approved for schools.

Beyond that, the Joint Fraud Taskforce has recently been relaunched and, through that, we are looking at having a television campaign to raise awareness. There are lots of different parts from different groups, some of it specifically targeted at people at risk and some of it more general education. There is quite a lot going on in that space.

Lord Browne of Ladyton: Thank you. Our other witnesses are welcome to add to the list of how you do it. I am interested in your assessment of the level of penetration and success. Do you have any data that you could share with us about the level of awareness among your respective customers and how you measure success in educating them? I am aware of this issue, yet I have no conscious recognition of ever having seen anything that said "Take Five" in any environment that I have ever been in, but I am not the same as everybody.

Brian Dilley: Various parts of the Take Five campaign have been targeted at particular demographics. There has been a more general

campaign for everybody, but there have also been some targeted things for specific at-risk populations.

On measurement, the awareness piece is the only reliable measure that we can really have. The issue with a retail banking customer is that if they have seen the Take Five message and hang up the phone on somebody, they have therefore been educated and we have stopped the scam. They do not phone us up and say, "By the way, I just hung up the phone". Reliable metrics as to what it has prevented are difficult, but my personal view is that it is the first line of defence, because the best scenario is that they hang up the phone.

With some of our commercial customers we have a bit more information, because where we have a relationship-managed customer we have seminars and things for them on individual risks to their business. When they are targeted, they often have a conversation with their relationship manager and explain that. We have a bit more information, but unfortunately for retail customers, measuring where we have prevented a fraud is almost impossible, so we have to have proxies for that and an awareness measurement to try to get to that.

Lord Browne of Ladyton: Thanks.

Nicholas Taylor: I will quickly touch on the warnings part and then on the data side, if that is all right. I will not repeat stuff that Brian said.

On the warnings, we have three main buckets. There are the prepayment warnings where if you add a new person you have never paid before we put a big, red screen up saying, "Do you know and trust this person?" There is confirmation of payee, but, frankly, customers are blind to that now because it has been around for a year or more. Then we have post-transfer warnings—when our models detect it—to say that it is 90% of these things. Those are incredibly explicit now. We have upped the punchiness, because they were not cutting through.

Now we have Instagram-style stories that customers cannot even skip through; we make them sit through them and we put in big, red text: "This payment is riskier than 99.3% of other Revolut payments", to really try to make it aggressive. We work with behavioural scientists and others on how we can do that. Then there is the normal customer education—email campaigns, push notifications and that sort of stuff.

On data, it is very difficult to measure. If it was a marketing campaign, we would have a control group, and we would not send marketing to them or any incentive to sign up a new customer, and then we would do A/B testing. We would give one group of customers £5 to sign up a friend and another group of customers £10, and look at the impact versus the control group that had no incentive. On fraud, we do not think it is morally right to have a control group where you do not send any warnings or do any customer education, which means that there is no counterfactual, so we cannot show causality. Perhaps the government Behavioural Insights Team, the nudge unit, could specifically lead some

studies on this, because as an institution we would not want to have a control group of customers who had not been sent warnings.

Lord Browne of Ladyton: You made an interesting remark about what you called an Instagram-style campaign. Am I right, or am I wrong, that if you were marketing, you would have a presence on social media in this environment nowadays? Do you have any presence on social media that young people use to try to get the message across to them? Do you employ influencers to try to change people's behaviour?

Nicholas Taylor: By Instagram-style, I meant that we have warnings in the stories on the app. It is very explicit. We also do paid-for advertising on those platforms to warn customers about scams and stuff. That touches on the online safety Bill, which we may get to later, where we were paying the tech platforms to advertise to warn customers about scams while they were profiting from criminals who were paying them to scam our customers. We really welcome the Government's move on that. Sorry, I am probably straying off questions. Yes, we do paid-for advertising to try to warn customers.

Lord Browne of Ladyton: I apologise, I encouraged you to do that. Geraldine, do you have anything you would like to contribute?

Geraldine Lawlor: On top of what the two gentlemen have already alluded to about what happens, there is a broader piece, not only from a personal institution perspective but supported through the likes of UK Finance at industry level. It relates to what you mentioned about not seeing the Take Five campaign and thinking about the UK's response. For example, there is the Economic Crime Strategic Board, chaired by the Home Secretary. It is whether there is the opportunity for a government-led narrative that all the industries can get behind and support, so that it is aligned to fraud being viewed as a national security risk and can start to play into that.

As Brian mentioned, prevention is surely the aim that we are going after. We want to protect the consumer from falling victim in the first place. If you can really strengthen that end of the equation, you have a much higher success rate in starting to interdict and take down fraud and the impact it has in harm and on the prosperity of the economy. Bringing in a government narrative that others can row in behind is important. It does not stop them running their own individual campaigns to belt and brace what they are trying to say that is relevant to their industry, but it would harness a consensus message to the consumer from UK plc in the round. I certainly think that could strengthen all the individual messages and campaigns that are being run by the different sectors.

Lord Browne of Ladyton: Thank you. That is very helpful. In other words, to normalise awareness we need to do this nationwide, and the Government need to get involved.

Geraldine Lawlor: Exactly.

Lord Browne of Ladyton: Thank you.

Q36 **Baroness Kingsmill:** Hello. As consumers are increasingly moving away from traditional banking styles and more towards a digital form of banking, do you think there are particular challenges for the digital banks in detecting and preventing digital fraud? Are there any additional tools and any additional challenges for the digital sector of banking?

The Chair: Baroness Kingsmill, do you need to declare something?

Baroness Kingsmill: I was the founding chair of Monzo, so that is probably important. I am no longer the chair, but it is probably important to say that. I am sure the Revolut people knew that.

The Chair: I am sure their research has shown it. Is your question for Nicholas in the first instance?

Baroness Kingsmill: In the first instance, perhaps Nicholas could clarify whether Revolut actually is a bank.

Nicholas Taylor: In the UK, we are licensed as an electronic money institution, whereas in the EU we have a banking licence via the European Central Bank. In the UK, we are not a bank; we are an EMI.

Baroness Kingsmill: It may not make any difference to your answer to the question in any event.

Nicholas Taylor: The only difference is in how safeguarding works and deposits, which is very boring and technical and I can get into that. From the customer's point of view, we are probably better placed on fraud. We are a tech company first and foremost, and we do financial services. Financial services companies can do our part in tackling fraud through machine-learning models and through detection and prevention. As I said, we have some of the best engineers in the world, and we have built stuff that can detect over 90% of fraud. We are a tech company first, so we are good at data and building models to detect fraud.

Baroness Kingsmill: What about the know your customer checks? How do those work? Do they work in any particular special way as far as digital banking is concerned?

Nicholas Taylor: It is very similar to others. In most high street banks you can sign up digitally now. When a customer does it, they put through their name and address. They have to have a photograph of their ID or their passport. We then have to have a 3D. It used to be selfies, but now it is videos; it is live stuff. Then we match them against each other, and they pass through the KYC checks and so on.

Digital KYC has been around for a while. We would like to see digital ID more broadly because we think it will be more effective and more secure. DCMS has been working on that for a while, and we would like to see it accelerated.

Baroness Kingsmill: What about voice recognition?

Nicholas Taylor: We do not do voice recognition. I know some of our competitors do. It is something we will look at. We are always open to other ways in which we can strengthen controls.

Baroness Kingsmill: What about the anti-money laundering issues that have caused some of the digital banks, including Monzo, some problems?

Nicholas Taylor: It is a thing that we, in the whole industry, take incredibly seriously and it is a constant challenge. Fraud is a predicate offence to money laundering. One firm's fraud is another firm's money laundering. We all have to work incredibly hard to try to detect, prevent and crack down on it. We do that through a two-pronged approach. We have former law enforcement officials from the NCA and others and former senior financial crime people from high street institutions, combined with the best engineers and technologists in the country to really crack down on this stuff.

Baroness Kingsmill: Revolut has had some challenges in this area, has it not?

Nicholas Taylor: Financial crime is an issue for the entire industry, as you said—for Monzo and others.

Baroness Kingsmill: I am not suggesting that it is anything special to you, but you have had experience of these challenges, and I wondered how they came about and how you dealt with them, because that will help us all to understand. How did it come about, and how did you deal with it?

Nicholas Taylor: Like others in the industry, we are a growing company. It is a highly regulated sector, and we work very hard to get these things right. We take feedback from regulators very seriously and improve. This is not an isolated issue for us. As you will have seen from the "Dear CEO" letter that went to the entire financial services industry, AML compliance is something that everyone needs to improve.

Baroness Kingsmill: Brian, would you like to respond to those questions in relation to the mainstream bank element?

Brian Dilley: It is not particularly different. We use AI and machine learning as well in anti-money laundering and fraud detection. We are a digital bank. Maybe we did not start there, but we are a digital bank now.

On your KYC question, we do electronic checks for KYC where we can, with somebody coming into a branch with their passport as a back-up as the exception rather than the rule. With some of that, it is much more effective because you triangulate the data to check that the person is who they say they are. You are checking in government sources—passport numbers, driving licence numbers—and going into electronic systems to find information that only that customer could know. When you match it against other information, it is much more effective than somebody walking in with what might be a forged passport. The online checks are more effective.

We have lots of analytical machine learning and AI models running across the different transactions and, as I said earlier, the behavioural aspects as well, to alert us. To give you an idea of the scale, we stop £10 million-worth of transactions a month for suspected fraud. That generally affects about 95,000 customers each month, so we are reaching out to 95,000 customers to say, "We need more information from you. We think this might be a scam", and trying to stop them being victims.

Baroness Kingsmill: What is your relationship with the police in these matters? Do you report every incident to the police?

Brian Dilley: We have a central database that feeds into the Action Fraud data. We do not report each one individually to Action Fraud, but we download our fraud data to the same repository that the Action Fraud data goes into.

The banking protocol is the best example of our interactions with the police. We were the pilot bank for it and introduced it several years ago. It is a scenario where, if somebody is in the branch and we think they are being scammed, we will, to start with, try to persuade them and try to explain to them what the frauds are, but if we think they are going to go ahead with it, and we still think it is a scam, we can call the police, who will come round. Sometimes, the presence of the police will shake them out of the hot state that I mentioned earlier. Other times, it is essentially a crime in progress, and the police are able to arrest the perpetrators.

The banking protocol has worked really well. We are about to roll it out on telephone, where it will work slightly differently. We work very closely with the police. As I mentioned earlier, as part of the City of London Police partnership that we have at Lloyds, we have funded an intelligence cell that looks at courier fraud. That is where somebody takes cash out and then a courier comes round and collects it from their house. The work that was done there in the targeted takedowns, as they call them, was extremely successful in arresting people involved in it. We work very closely with the City of London Police in particular as the lead force for fraud and cyber.

Baroness Kingsmill: Fraudsters can be very creative. Have you noticed trends, and do you keep a record of the different trends in fraud?

Brian Dilley: Yes, we share across the industry. We make changes to our monitoring on a daily and hourly basis. As soon as we get a rule or a machine-learning tool that is working, they will adapt and move away from it. The confirmation of payee movement is probably the most significant in that you can actually watch the change in fraudsters' behaviour. Our analysis in Lloyds suggests that it is 100 times more likely to be a scam going to a non-confirmation of payee bank than to a confirmation of payee bank.

UK Finance has just done some preliminary analysis of the money flows. It has identified that 50% of scam proceeds go to banks that do not have confirmation of payee, and those banks represent about 5% of the

number of payments. As soon as confirmation of payee came in, there was a migration to people who do not have confirmation of payee. That was within a week or two. We invested a huge amount of money in putting confirmation of payee in and they moved to the banks that had not done it, or rather to the institutions—the payment service providers—that had not done it. That is quite a good example of how quickly the fraudsters adapt.

The Chair: Brian, on your point about confirmation of payee, would you and other banks that are part of confirmation of payee like to see all institutions having to be part of that?

Brian Dilley: Yes, definitely. It has worked well. It is one of the things that shakes people out of the hot state because you look at something and say, "Hold on, that's not matching". At the moment, those who do not have confirmation of payee get a warning: "We are unable to verify it and it is up to you whether you proceed". Yes, absolutely.

Nicholas Taylor: I agree. We were not forced to do it, but we have had confirmation of payee for a couple of years. There is no reason why any firm operating in the UK should not have confirmation of payee.

The Chair: Thank you both. That is very helpful.

Q37 **Lord Vaux of Harrowden:** I want to ask about the ways in which fraudsters receive the money, which seems to be a critical element in the pathway. I am afraid it is another three-part question, if that is okay.

Money mules have been mentioned a few times in the evidence so far. First, could you explain what money mules are, who they are, how they are recruited and what we might be able to do about that? Secondly, what has been the impact of faster payments on fraud? Would it make sense to try to slow down fraudulent transfers in some way, and how might we do that? Thirdly, what has been the impact of cryptocurrencies, and is that now becoming an issue in fraudsters taking money?

Geraldine Lawlor: Mules are where somebody uses another person's account to transfer money into. We have seen in the market different ways in which they have been recruited. Brian alluded to a couple of them in his first answer. There are different types of mules in terms of when they are recruited. We have seen examples where a student account could perfectly transact and operate normally, but when certain foreign students choose to go home three years into the account being held, or the relationship, it suddenly starts to convert into a mule.

In a former role I was in, we would see fraudsters hanging around universities and looking to engage people to sell on their account, viewing their account as no longer of value to them. There are different ways by which organised crime engages with people and dupes them into allowing their account to be used in that manner. What we have seen in that particular area is the real benefit of using analytics to identify through trends the different profiles and categories of mules, and the propensity for when accounts are likely to become a mule account. We are then able

to apply controls to such accounts to interdict them when we see an unusual credit coming into the account. There are different means by which the banking industry is able to identify that and help to put controls into play.

One of the challenges of faster payments—my colleagues will expand on these—is that they are almost straight-through processing. They enable fast movement across the system of transfer, and should be viewed almost as a means of cash. The challenge is that the ability to interdict and investigate such a transaction is very difficult to align to meeting your PSD requirements. As a result, there is certainly a view within the industry that the ability to interdict is very valuable, particularly in the investigation of what one understands to be a fraudulent payment and proceeds of crime, and then to be able to react accordingly. I mentioned the mule situation before; some banks have been able successfully to put in those controls to stop a payment mid-flight, investigate it quite quickly and make a decision quite quickly.

When I worked in Barclays, we were very successful at both taking down our exposure to mules and being able to interdict on fraud on the credit and repatriate funds to victims. As a result, the industry is starting to look at very similar principles—to go back to what Brian and Nicholas alluded to—in sharing best practice. We are starting to think more broadly about how the industry as a whole can start to apply similar principles, through propensity modelling, to identify potential mules and interdict on the credit rather than traditionally what was done on the debit side when money has gone from the system.

In the industry, there has been a lot of conversation around putting some friction back into payments, and for the ability to stop and investigate, particularly if the first level of controls, such as prevention, education and awareness, has failed and the customer has made the payment regardless of attempts by the industry to stop them. You need to be able to put controls down through the value chain so that you can interdict as it keeps going through. Certainly, that is one way on faster payments.

We are seeing a move of funds into crypto, but the industry is able to monitor for where we see conversion from fiat to crypto, and in some cases is able to interdict at that point, and stop and question, not just in the live situation but after the event. We are able to pull information through and start to identify where potential individuals are moving money out of the system and ask questions at that point. There are examples across the industry of recognising the trend and the movement, and where controls are starting to be assessed as to how to intervene at that point.

Lord Vaux of Harrowden: On the mule side, what can we do to make it harder for mules to be recruited? You mentioned them being duped. Should we be looking at mules as victims or as criminals?

Geraldine Lawlor: There are both. There is a piece definitely where we talk about education to the consumer to prevent them being a victim.

There is a similar need for education for individuals to stop them becoming viewed as a criminal for allowing their account to be used in that way. The long-term impacts are that they will find it difficult to get credit or anything of that nature as they continue on their life path, and want to get facilities or access to loans or money in the future. They need to know the implications of allowing their accounts to be used in that way. Education is just as important to that sector as it is to the consumer, because it is all about prevention. There are mule herders out there who are aggressively doing this and are very professional at doing it, so if you can stop mules being hired, you can stop people being duped into giving access to their account. It has a positive impact on prevention as well.

There definitely is a role for education at that level, just as much as there is on the consumer side. As on the consumer side, sometimes individuals do not take heed, and they still allow access to their accounts. There is a point where you can determine that they have been reckless and have ignored all the attempts to prevent them going down that route and have gone ahead regardless. That is assessed in how you determine whether they should be treated as a criminal or a victim.

Lord Vaux of Harrowden: Are there particular platforms that fraudsters or mule herders are using for recruitment purposes? You mentioned people hanging around universities, so there is a physical element, but presumably quite a lot of this happens on social media or in gaming. Are there any particular trends?

Geraldine Lawlor: I might pass that to Brian or Nicholas, who might have a better view on it, if you do not mind.

Lord Vaux of Harrowden: Okay, let us move to Brian. Is there anything you want to add? If you have any views on the last question, that would be great.

Brian Dilley: Mule herders openly advertise on social media across numerous platforms, which is why we would like more monitoring and takedown of those services. They get taken down when we notify the social media companies, but we would like them proactively taken down rather than just taken down on notification.

More generally on education of the mules, part of it is understanding what will stop them doing it. The anti-fraud agency, CIFAS, did some research a couple of years ago at universities, where they said, "Do you realise what the money you are passing through your account is funding? It's funding human trafficking". Some people said, "I didn't realise that", and that would stop them doing it. CIFAS went through the different levels: "Do you realise you might not be able to get a bank account?" Some people said, "If I might not be able to get a bank account, that might deter me". The one that really resonated was, "If you don't have a bank account, you won't be able to get a mobile phone contract". All of a sudden everyone was worried. There is a bit of targeting the education to the things that mean something to the people you are trying to talk to.

As regards what the banks can do, we introduced a mule hunting team back in 2017, which has been very successful in looking at incoming payments. A lot of the anti-money laundering transaction monitoring is post event; the money has already come in and gone by the time you detect and report it. We introduced real-time intervention in the mule hunting team, and since 2017 that has frozen £60 million of proceeds going into customer accounts, often genuine customer accounts that were allowing money to go across them but also some controlled by criminals. Where those are fraud proceeds, we are able to give the money back to a victim who is a customer of another bank. We then shared that system with the other banks. A number of them have adopted it and said, "If we all do this, we can give money back to the victims who are our customers".

My last point is on your question on faster payments. We are working with government and regulators to try to define and agree the circumstances where we can slow down payments. To give you an idea of what we are required to do by legislation and regulation at the moment, faster payments have to be immediate, which is defined by the FCA as within two hours. There is an argument that we can delay it for a day if we are looking at something we suspect, but a day is not a very long time. It also assumes that there is somebody sitting at your detection machine waiting for the next one to come off the rank, and that they will pick it up the instant it comes in and then your two hours starts, which in an operational environment is not the case. Slowing down faster payments and the ability to talk to the other bank, get information from the other bank, talk to the customer and involve the police where necessary would make a big difference.

Lord Vaux of Harrowden: Is there anything stopping you talking to the other bank?

Brian Dilley: We can talk to the other bank, and we do, and we can get a certain amount of information, but the other thing we are looking for in the economic crime Bill—the second economic crime Bill as it is now—would be more powers to share more information. GDPR and the data protection legislation have an exemption for fraud, but it is still fairly limited and not every bank has the same view of what it can share, or the same risk appetite for some of the civil liability that might come from sharing information on their customers.

The difference with fraud is that if you are talking about a fraudster, sharing information about a fraudster that is external to the bank is not sharing information about your customer. If your customer is a genuine customer who is a mule, what information can you share about that customer with the other bank? Different banks take different approaches, because it is not clear what you are able to do and what you are allowed to do. We share information, but we are restrained. Different banks share different amounts of information, so we would like to get that clear.

Q38 **Lord Allan of Hallam:** I want to dig into this with a question particularly for Brian and Nicholas. The two of you represent institutions that

presumably have good databases of attempts of fraud, money mules, et cetera. What are you able to share with each other today, and what is needed? Brian, you mentioned some comfort around GDPR and some common standards. What do you need practically? I would have thought that the ideal state was that you very openly and willingly shared data with each other and all the other institutions about people who are trying to scam your customers.

Brian Dilley: Absolutely. We do not have any issue about sharing, and we share information on typologies, trends, people who are targeting our customers, people who are launching smishing attacks, et cetera. Those are things that are external to the bank or to the institution, so that is not a problem. The difficulty comes when we are sharing information about our customers where they are involved in some way. If they are actively involved, if we think our customer is a criminal, we generally take the risk of sharing the information with the other institution, but different banks have different appetites for that. The key for me is sharing information for the purposes of detecting, rather than telling other people something that you have already seen.

A few years ago, we did a good piece of work with the other banks when a fraudster was targeting all our customers with smishing attacks. We were trying to share information about IP addresses from our customers who had accessed their accounts from various IP addresses in order to try to match them to the fraudster and identify who it was. That was a good example where some people said, "I have 20 customers who have logged in from this IP address"—IP addresses are reused—"and 20 of them might be innocent, so I'm not sure that I have the power to provide the information centrally that would enable us to find the fraudster". The more you go into the data about genuine customers that you are trying to share for the purposes of identifying trends, the harder it is and the bigger risk you take as a financial institution.

Lord Allan of Hallam: Thanks. Nicholas, as a modern bank, I assume that you are into sharing as much as you can. You are at the risk-tolerant end.

Nicholas Taylor: Yes. We are very willing, and we share data bilaterally. My colleagues in our data protection legal team, whom I can see sitting over there, spend hours and hours trying to sign bilateral data protection arrangements with other firms. As you know, there are different ways in which you can share data under the Data Protection Act. The one we rely on in this instance is legitimate interest. It is in our legitimate business interest to detect and prevent fraud.

As Brian said, it is a matter of risk appetite, and some institutions are very hesitant in this space. Although we take the view that we are able to share this stuff under the legitimate interest test, what would give those other firms more comfort is explicit guidance from the Information Commissioner's Office stating, "This is an example of a legitimate interest. It's fine". If you wanted to go one step further, it could be explicit in secondary legislation that examples of legitimate interests are

the examples given there, "but not limited to, sharing data for fraud". For us, the easiest thing and the one that we think would be most effective and quicker would be getting the ICO to issue a public statement or guidance on what is of legitimate interest.

Lord Allan of Hallam: Thank you very much.

The Chair: That is very helpful. Thank you very much.

Lord Browne of Ladyton: This is a direct supplementary about risk appetite and whether the concern that people have about it is a reality. It is a simple question to you, Nicholas. You seem to have a bigger appetite for risk in this environment than others may have. Has this been to your detriment? Have you been flooded with civil litigation from people who are unhappy about the fact that you are protecting your customers from fraud?

Nicholas Taylor: No.

Lord Browne of Ladyton: Thank you.

The Chair: That was a perfect short answer. Thank you very much indeed.

Q39 **Baroness Bowles of Berkhamsted:** I want to explore a little bit about the contingent reimbursement model code, which we have had since 2019 and at the moment is voluntary, although the Government have promised that all banks should have to sign up mandatorily. One thing I noticed when it appeared—maybe it was coincidence—was that there were simultaneously a lot more questions when you tried to make a payment, warning you, "Do you know who this person is?" My suspicious mind then thought that it was to be able to prove that it was not reasonable to expect me to make that payment.

How do you deal with what is and is not a reasonable point? Should the statistics on reimbursements of victims by bank and the reporting of rates of reimbursement be mandatory, so that the public know what their chances are with given institutions?

Geraldine Lawlor: First and foremost, the code has been quite successful. UK Finance figures show that £147 million of losses were reimbursed in 2020, so it is certainly having an effect.

You asked about measurement. Measurement is always helpful in a system, because at least you have something tangible to reflect on and can look at trends year on year, but there are sometimes unintended consequences with measurement, particularly as numbers in and of themselves lack context for cases that were reimbursed and, more importantly, cases that were not. If you look at pure numbers, sometimes people compare across institutions. It may not give you the full context and it could drive the wrong outcome and behaviours. It could also lead to people wanting to drive up more or even down, or even question their own framework if the numbers do not compare. Regulators use these

types of measurement to try to compare institutions, when actually they are missing the context that sits behind them.

Looking at the CRM, the code, in itself, and the question of whether everybody should comply with it and it should be mandatory, absolutely. Then we need to consider what type of measurements would be helpful to drive the right outcomes in the system, while being cognisant of not driving the unintended consequences of measurement in some cases, particularly when it is just on bare facts, such as the value of reimbursement aligned to those that were not reimbursed. That is the first piece I would be cautious about.

Baroness Bowles of Berkhamsted: I cannot help but think that figures that show how often customers of certain banks are scammed are relevant. I realise there are different sizes. If you know that 50% are scammed in one bank and 10% in another, or that 50% get reimbursed in one bank and none in another, those kinds of figures are relevant. They may not be exact, but they are relevant.

Geraldine Lawlor: They are if the context is added. Sometimes they may not be reimbursed because the number of frauds is low and the controls are stronger in that particular institution. It is trying to understand how you can compare the numbers on a like-for-like basis rather than on a pure number basis. That would be the only caveat I would put to it. I agree that measurement is helpful, but it needs context to make it meaningful as well.

Baroness Bowles of Berkhamsted: You could put around it the percentage of times that things went to the financial ombudsman and the percentage of times that the financial ombudsman overturned what the bank had done and said, "No, you should reimburse".

Geraldine Lawlor: Yes, along with why.

Baroness Bowles of Berkhamsted: Indeed. I have a slightly different question, not so much to do with the code. Some people suggest that more could be done by banks against fraud, but they accept a certain amount as the cost of doing business. Would you say that that was true? What additional steps might be taken if, as with bribery, you have to show the steps you have taken, otherwise you offend under the failure to prevent offence? Would a failure to prevent offence, as many suggest, help out and make banks do more? Obviously, there are good banks and less good banks. Would it make the laggards step up more?

Geraldine Lawlor: It is challenging when you listen to some of my colleagues on the different controls that have been put into the system all through the pipe for how to really support on prevention by educating the consumer, as well as the controls that have been put in place to detect and report. The challenge with fraud is the extent of it in the system, and the fact that as soon as you put controls in, it moves into another guise and moves off to the weakest link. It is very challenging to apply a failure

to prevent when institutions have applied controls to the system in relation to the fraud that is hitting them at that moment.

There is a tolerance level that definitely has traditionally played into this space, where certain institutions were willing to accept a level of fraud in the system, versus where it is today, which is that it is so endemic across the whole system that looking at how to manage it has become very challenging. As a result, it has come right up the institution in prominence and importance, because what was traditionally a P&L write-off is now too extreme and is no longer tolerated to that level, so it has required a different response, and it is getting a different response.

Looking at it under failure to prevent is quite challenging in terms of what it will drive in practice in institutions, and the cost as part of that. It tends to drive controls into the detection end, as opposed to how you move it up stream to support prevention, because that is the only way to bring it down and out of the system. That would be my initial view in relation to that. I am keen for my colleagues to contribute to that question.

Brian Dilley: There is an awful lot going around in my head, but I am conscious of time. At Lloyds, we do not treat fraud as a cost of doing business. We have invested over £100 million over the last three years in our fraud detection system. I do not think a failure to prevent offence would make a difference to how we treat it.

We think there should be a mandatory code, not necessarily the code that is there at the moment. It has been successful, but the recipient bank is almost never held liable under the code, and the level of consumer care, which goes to the education point and protecting yourself, is generally held to be much lower. We need to focus on prevention and stopping the criminals getting the money more than on reimbursement. I agree with what Geraldine said about the unintended consequences and the misinterpretation when publishing data in those scenarios.

Nicholas Taylor: I will be very brief and I will not repeat the other stuff. Focusing on reimbursement is important, but ultimately reimbursement is treating the symptom. We need to tackle the root cause. Ultimately, payment service providers are the final step in all of this. We need to drill down and focus on those who bring risk into the system. That is my view.

The Chair: Thank you.

Q40 **Lord Gilbert of Panteg:** Witnesses, I want to talk briefly about how you work with the Government. We have had a whole alphabet soup of Whitehall acronyms for initiatives and forums that have taken place to bring the industry together with the Government, but the one that comes through most frequently is the Economic Crime Strategic Board. Brian, I think Lloyds Banking Group sits on it. Nicholas, I think you are represented on it by UK Finance.

Perhaps I can start with Brian. How do you find it? It is supposed to be led by the Home Secretary and Chancellor. Do they lead it? Do you sense

that they are driving it? How often does it meet, and can you point to any single tangible success that the board has seen?

Brian Dilley: The Economic Crime Strategic Board is the top-level committee, or group, that meets in relation to the Government's economic crime reform programme. It is fair to say that it has met irregularly. Largely, it has suffered from changes in Ministers, Brexit, the pandemic, et cetera. When it has met, it has made a positive contribution. It sets the strategic direction. It agrees the priorities. A key deliverable from it has been the development of a fraud action plan, which is due to be published later this year. It came about from a discussion about economic crime reform. When it started, it was probably much more focused on money laundering and not on fraud.

The Economic Crime Strategic Board was where we said that we needed to focus more on fraud and agreed to develop the fraud action plan, and that is now in operation even though the plan itself has not yet been published, but it is working. The Economic Crime Strategic Board is a force for good. It has been chaired by Home Secretaries and Chancellors along the way. The intention is to have it meeting regularly now. It has suffered from a number of things that have thrown it off course in the last two or three years.

Lord Gilbert of Panteg: It has not always been chaired by the Chancellor or Home Secretary.

Brian Dilley: I think it has, has it not?

Lord Gilbert of Panteg: It has always been chaired by them?

Brian Dilley: Yes, I think it has.

Lord Gilbert of Panteg: Okay. On the issue of Whitehall responsibility, who would you say is the lead politician in Whitehall—the lead Minister in Whitehall—bringing all this together into one coherent strategic approach?

Brian Dilley: The answer to that is there is not currently one, and that is one of the things that we want for fraud and for economic crime. We often talk about it as system leadership. We have a number of active Ministers. Apart from the Home Secretary and the Chancellor on the Economic Crime Strategic Board, probably the two who are most active are the Security Minister and the Economic Secretary to the Treasury. We, as a group of banks, have been having regular, slightly less formal meetings with them for the last few months, which is really making a difference. It is not a committee meeting with lots and lots of papers; it is a discussion. That is where we have started to make progress on developing proposals to slow down faster payments in certain risk-based scenarios. System leadership is critical, because there are lots of different Ministers from lots of different departments, all with conflicting priorities. If we had system leadership, it would make a massive difference.

Lord Gilbert of Panteg: Okay. Nicholas, you are represented by UK

Finance. Does that relationship work? Do you get any value out of it through UK Finance?

Nicholas Taylor: Yes. Our chief risk officer attended the last Economic Crime Strategic Board. The representation is improving and getting better at having digital firms at the table. I echo the point that Brian made. There are a lot of departments, a lot of officials and a lot of acronyms involved in this space, and it is sometimes pretty confusing as to who to engage with, particularly for some of the newer challenger firms like us. Obviously, we have the Home Office and the Treasury. When we talk about intelligence sharing, it is a DCMS and ICO responsibility. I would support the call for a single Minister, but ultimately it is not for firms like us to opine on machinery of government changes.

Lord Gilbert of Panteg: Except that Ministers are always urging you to get your act together and work together effectively to co-ordinate industry responses, so it seems reasonable that we should be telling Ministers to get Whitehall to co-ordinate and join up. Geraldine, shall I come to you on that? What is your observation across the industry on the multiplicity of forums? Do you think it is getting anywhere near being joined up? If it is not, what is the price we are paying?

Geraldine Lawlor: The attempts to join it up are definitely there, but it is not by design. It is almost where the industry recognises, along with government, that this needs a co-ordinated response. A lot of the stakeholders are coming together to look at that and support it. The economic crime steering committee was put in place to help initiate that and create the tone from the top, with the leadership piece coming out of government, even bringing CEO representation to it. We see that filter down in things like the Joint Money Laundering Intelligence Taskforce, the fusion cell, the Joint Fraud Taskforce, just to mention three.

There are other initiatives. It is almost the actors in the system going about attempts to bring it together, sharing intelligence and sharing best practice, rather than how the system is designed, that is creating the best benefit. It has proven the hypothesis that working together really can strengthen the system as a whole and strengthen the individual players within it. If you have proved the hypothesis, let us put it into practice in a framework that is enabled through the right legislative reform and supported by the right structures in place, and, as both Brian and Nicholas mentioned, leadership from within government that brings it all together.

Lord Gilbert of Panteg: Thank you.

Q41 **Baroness Henig:** Good morning. Pursuing the theme of collaboration that Geraldine has just outlined, and talking specifically about the Joint Fraud Taskforce, how are your companies working to meet the commitments made in the fraud sector charters? Presumably, that is one way in which you can co-ordinate action across the piece. I think Brian mentioned a television campaign, and I was not sure whether it was in this context or not. Perhaps we could hear something about that.

Brian Dilley: Yes, it was in this context. The Joint Fraud Taskforce was relaunched last October with a ministerial chair, which is a really good step forward. We are fully engaged in that. We sit on that group. The campaign is part of the discussion there as to one of the possible things that might come out of that group.

On the sector charters, the banking sector charter in particular is quite a small subset of what we are doing as a banking industry and how we are working together. A lot of the things in the sector charter are led by UK Finance, and we are fully engaged in providing the data and information for that. UK Finance has a new stand-alone project on fraud that we are all contributing to. The activity we are doing for that, which is an awful lot of attribution sharing—information sharing in real time—will be more effective than some of the things in the charter. The charter is one of the key things that we are delivering partly to try to measure in a better way the success we are having with the other activities we are doing. The work is progressing, but I would not say that the sector charter is the be-all and end-all of what we are doing as a banking sector. We are doing an awful lot more that will have bigger impacts as well.

Baroness Henig: Geraldine, do you have anything to add?

The Chair: We have put it to the companies, so shall we ask Nicholas about the charter?

Nicholas Taylor: I have nothing to add. I am conscious of time, so I will stop.

The Chair: All right, that is great. We are briefly moving internationally.

Q42 **Lord Sandhurst:** Fraud does not respect borders. A credit card can be cloned in country A and used to make a remote purchase in country B, to take an example. How do financial companies work with regulators and global banking partners to tackle this cross-border activity? What structures are lacking that you think might improve things?

Brian Dilley: One of the challenges, particularly of investigation and prosecution by law enforcement, is the international dimension, because the incentive and the product of an investigation might not have a prosecution at the end of it if they are not in the jurisdiction. We share information internationally. It is not as good as domestically, to be honest.

The area we need to focus on is preventing some of the entry to the UK system—for example, telecoms companies preventing the phone calls coming from abroad that wil try to scam people, or the number spoofing where a phone call that is coming in looks as if it is from your bank or looks like a UK number. Those vulnerabilities are the biggest thing for us internationally. We work with agencies in other countries to try to persuade them to take those down, but our reach is a bit less effective in that scenario. It is about defending the borders in a digital way to stop things coming into the UK that look as though they are generated within the UK.

Nicholas Taylor: We have a good perspective on this, because we are a British company but we operate globally. The UK is about 20% of our customer base, but it represents about 70% of our APP fraud. APP fraud is a very UK-centric problem, but it is targeted from overseas. We cannot share data, so we cannot see specifically where it is going. We see UK customers being scammed and sending money to another UK bank or payment institution. It then goes, perhaps through a mule, to someone overseas, but we cannot see that hop because of the data-sharing points that we discussed earlier. We know that it is coming from overseas, but we cannot see specifically where because we can only see one hop, which is a UK customer being scammed and sending it to a UK mule, and then it goes abroad. A really important point is that APP fraud is a very UK-specific problem, so it requires an urgent UK solution.

The Chair: That is very helpful. Geraldine, do you want to add on the international thing before we wrap up?

Geraldine Lawlor: The only thing is on the whole approach to public/private partnership. It was initiated in the UK through JMLIT and has broadened out. International banks have a role to play, particularly where they have presences in other jurisdictions, to help influence the setting up of similar partnerships.

The UK was a leading voice in that. A couple of banks worked with the NCA to establish things like FMLIT in Hong Kong and helped to influence things like the Fintel Alliance in Australia. FELEG, the Five Eyes law enforcement group, has invited the private sector to be part of a number of its working groups, to bring public/private conversations together. Notwithstanding the individual cases that Nicholas and Brian alluded to, the private sector can play a role, because of its global networks, to help to establish some public/private partnerships in other countries and share insight and intelligence.

The Chair: Thank you very much. In a moment I will ask each of you to give us one key recommendation that you want to give the Government.

Nicholas, I cannot leave your comment about how much APP fraud is a UK-specific thing. Have we probed that sufficiently this morning? Is there anything else you want to say about why you think the UK is such a hot market for APP fraud that we have not covered this morning?

Nicholas Taylor: There is no simple answer. Frankly, we do not know. There are a few factors. Organised overseas criminals know their own language and English, so they target the UK. The UK public are very trusting of the internet and use it a lot.

Going on to the policy ask, it would have been the online safety Bill and advertising, which is very welcome. Because the UK public use the internet more and trust the adverts they see on the internet more, there is a higher propensity to be scammed like that. It also has to do with reimbursement rates. There is very high reimbursement in the UK, so frankly it is easy money for criminals.

The Chair: That is very helpful. If there is anything after this session that occurs to you particularly on that—

Nicholas Taylor: There is more data I get on the international side that I do not want to put in the public domain.

Q43 **The Chair:** Okay. We would be very happy to see that, and perhaps we can discuss access to that data offline.

If there is one recommendation that you would like to make to the Government, or would like us to make through our report, we would be delighted to hear it.

Brian Dilley: Mine would be a whole-system approach to prevention: single-system leadership with all parties that bring risk into the system working together, with the ability to share information to stop the criminals getting the money rather than focusing on reimbursing customers after it has happened, which we need to do as well, but it should not be the main focus.

The Chair: Thank you.

Geraldine Lawlor: Brian covered a number of points in that one. One other piece is government co-ordinated action on messaging to the consumer, with government taking the lead on that, so that there is a common voice coming from UK plc on prevention for consumer protection.

The Chair: Thank you. Nicholas, one recommendation. We have done advertising.

Nicholas Taylor: It would be for the ICO to issue statutory guidance that sharing data for fraud is a legitimate business interest.

The Chair: Thank you all very much indeed. I am conscious that we have kept you a bit longer than planned. It has been a fascinating session and very helpful for our next session, which will follow immediately after this.