Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 26 May 2022

9.30 am

Watch the meeting

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

Evidence Session No. 14 Heard in Public Questions 146 - 159

Examination of witnesses

Mark Steward, Chris Hemsley and Huw Saunders.

Q146 **The Chair:** Good morning and welcome to this session of the House of Lords Select Committee on the Fraud Act 2006 and digital fraud. We are delighted to be joined by the regulators this morning. Thank you to Mark Steward, who is the director of enforcement and market oversight at the Financial Conduct Authority, Chris Hemsley, who is the managing director of the Payment Systems Regulator, and Huw Saunders, who is the director of network infrastructure and resilience at Ofcom. Thank you all very much indeed for being here in person this morning. This is a hybrid session. We have Baroness Bowles and Lord Allan online as well.

I will kick off with a question to all of you. How do the regulators, all of you, work together to prevent scams across the fraud ecosystem? Is that collaboration effective? Are there things that could be done to improve it? Mark, I will start with the Financial Conduct Authority.

Mark Steward: First of all, we work broadly with both regulators and law enforcement. It is a combined effort through things like the National Economic Crime Centre, which has been established, housed in the NCA, and the Joint Fraud Taskforce. Those enable us to work in combination.

There are also some unique regulatory initiatives that I am sure Huw will also mention, such as the Digital Regulation Cooperation Forum, which is the FCA, Ofcom, the CMA and the ICO. The Digital Regulation

Cooperation Forum published a workplan just last month that described the work that the FCA and Ofcom were going to do together on illegal financial promotions under the proposed Online Safety Bill as well as looking at the wider work the FCA can do with the ICO.

That is how we work. How well does it work? I do not detect any reluctance about working together. There is an enormous amount of good will to try to get things done together and finds ways to collaborate together. It is part and parcel of the FCA's strategic plan, which we announced a couple of months ago, to see collaboration both with other regulators and with law enforcement in particular. That is the real key to making some progress in this space; that is not just in this space, but certainly in this space.

One point I would make about that is that everybody is stretched. From a regulatory perspective, everybody has to fit within their statutory remits. Those remits do not always line up side by side. There are gaps and there is no overarching regulatory architecture to which we all belong to. That has particular resonance when we consider the issue of fraud, because we know fraudsters are great innovators; they look for these gaps to exploit them.

Where there are gaps, there are blind spots. The challenge we face is in trying to identify those blind spots as best we can and working out strategies and ways to deal with them, given that we cannot change our own statutory remits.

The Chair: We will come back and probe some of those gaps. If, at the end, we have not identified all of them, you can help us to fill that in. I know Baroness Henig is going to talk about law enforcement particularly in a moment, so we will save that. Chris, how does the PSR fit into the regulators working together?

Chris Hemsley: I would also just echo Mark's point: the will is there. We always want to do this better, but there is definitely never a sense of reluctance to co-operate. I have met with the NECC as well to make sure our work is joined up there. We work very closely with Ofcom and the FCA.

It might be really useful to highlight an example. I know the committee will be aware, but we have been doing a lot of work on the prevention of authorised push payment fraud. As we have brought forward our proposals, that includes collecting more data. That is with a view to publishing it as well, but we have been collecting more data so we have a better picture of where problems are. Of course, that helps create the data that the FCA can use to be even more informed about where the issues in supervision are.

We are in the same building; we co-operate on a day-to-day basis. It really has an impact. We join up across those boundaries. As Mark was saying, the criminals do not respect these regulatory boundaries, so we have to make sure we join up.

The Chair: How does Ofcom fit into the picture with the regulators?

Huw Saunders: To be honest, there is not much I can add to what my colleagues have just said. There are mechanisms that are now in place. The DRCF is the most obvious one.

I would also stress that the Joint Fraud Taskforce, which has been revamped—that is perhaps the best word to use—over the last 18 months, is a really effective umbrella to look at some of these issues overall and address some of those gaps. They have introduced voluntary sector charters in telecommunications, tech, finance, et cetera, which the industry has broadly supported. The regulators have oversight of those, and there are groups being formed across industry, including via the NECC, to help make sure they are effective in terms of their delivery.

I would reiterate the point that scammers and fraudsters are extremely innovative. We put out a package of documents in February that was a demonstration of the complexity of one of the most common scams at the moment, the missed delivery scam. It looked at how many different aspects of different sectors are involved on an end-to-end basis before the fraudster is successful and gets somebody's money. That points to the fact that this is cross-sectoral. There needs to be regulatory oversight from a variety of different bodies. Equally, there are different industry sectors that all need to be involved in trying to mitigate the harm and prevent it from happening in the first instance.

The Chair: Exactly, yes. We want to get to the nub of that.

Q147 **Baroness Henig:** I want to probe into this very unwieldy structure that you are already beginning to describe. If we look at the relationships between the police and wider law enforcement and yourselves, there are two areas that are interesting to me. One is the number of organisations that are involved. How does it work? There are so many of you all dealing with the police and wider law enforcement. Is it effective? Can it work better?

My second issue arises from something that was said at one of our sessions last week with the big digital companies. They were going on about the difficulties of sharing data. They were saying that they could not operate with the police effectively because they could not share data. I was quite interested in this point. It was not universally agreed; shall we put it that way? The difficulties appeared to be on their side; others were not sure they actually existed. Could you comment on both of those aspects?

Mark Steward: On the first issue, how do we navigate the numbers ourselves? We are used to it. That is the first answer. This is relevant to the first question that was asked about how the regulators work together. In reality, we are not just working with one another. We are working with the police; we are working with the NCA; we are working the National Economic Crime Centre; we are working with the different police forces.

It is a much more complicated picture, but that is where the co-ordinating focus of the National Economic Crime Centre—the NECC, as we call it—really works well and is important. The NECC is in a position to bring together and has brought together both law enforcement and regulators. The FCA is a foundation member of the National Economic Crime Centre. We second staff there, we work closely and we are great supporters of the purpose and function of the NECC. It really needs more funding.

A key aspect to the need for co-ordination is the co-ordination around intelligence that we all have. That is not easy, and it is not cheap either. It needs real resourcing and infrastructure. There is some there, of course, but it needs a lot more in order to be really effectively. That would be my answer to the first part of your question.

The second part about the sharing of information is connected to this challenge we have around getting the right intelligence and getting a strategic view of what that intelligence amounts to. There are some issues around the extent to which the technology companies are prepared to give us the information we need. Often the response is, "It is not in the UK. If you need it, you need to ask another country to give it to you". That is not a sufficient response. That is a really big reason why the Online Safety Bill is so super-important. We do not need excuses; we need some powers to get the information we need for our purposes.

Chris Hemsley: As Mark has just talked about, there are well trodden interfaces. Another aspect of this is the fact that there are areas where there is a known task and we just have to focus on it. From the PSR perspective, we have these payment systems. What can we do in this space to contribute to the fight against fraud? Yes, we do need to join up, but there is a degree to which we just need to get on with our job in our area as well. That has been one of the features we have. We have to make sure we are all joined up and we are looking for those opportunities, but we have to see what we can do in our space.

I do not have too much to add on the information-sharing issue. I would just recognise that it is one of the themes that we have been pushing. It has not historically been a major problem; we have not wanted there to be more sharing of information. One of the particular initiatives that we pushed forward to improve the security around payments was confirmation of payee, which is a name-checking service that you may well have used. Behind that, there was a need to share information. We worked really effectively with the Information Commissioner's Office to make sure it understood what we were trying to achieve and why. That has gone live.

It can be complicated, but there is a risk that we do not use the law. It does not prevent the sharing of information when there is a good reason.

Huw Saunders: Picking up on the information-sharing point first, I would reiterate the point that in the telecoms environment, for calls and texts, et cetera, there are certainly instances where concerns are

expressed about privacy. The ICO has already issued formal guidance to explain what is allowable and is extremely supportive in terms of looking at particular areas where information-sharing perhaps is in a grey area. It will help people share information if there is a good reason why it should be shared, such as to prevent crime and mitigate harm.

The other thing that is worth noting is information-sharing between different sectors. I would point to the work of Stop Scams UK as an example of this. They are promoting co-operation between the finance sector and the telcos in terms of know your customer and things like that. If something happens to a particular telco customer—I am thinking in particular of so-called SIM swaps or issues related to the porting of numbers—information could be made available to the banks so they know there is something to be aware of, if there is a big transfer related to that customer at a particular point in time. That is quite effective at addressing that particular issue. It is an example where it is not just information-sharing between telcos or banks but between the different sectors that is specifically aiming to address these problems.

Going back to the law enforcement issue, we are equally involved with the NECC, which has proven very effective at identifying the right ways in for various issues that need to be flagged to law enforcement. The City of London Police has a primary role in this, and we have a direct relationship with them as well. I would also note that the National Cyber Security Centre plays a good role, particularly in taking down malicious websites. They are integrated into that process.

Q148 **Lord Browne of Ladyton:** This does not directly follow on from this question, but it is to me a fairly fundamental question. All of your organisations have an operational objective to protect consumers. I have no doubt that you all have operational priorities that usually include this issue and the prevention of it. There is a fundamental commonality here. The evidence we have received overwhelmingly shows that the people who know where the blind spots are, the people who can find the weak spots and the blind spots quickly, are the scammers. They are either there before you or, when you get there, they very quickly find ways of circumventing what you have done.

It seems to me that there is a question about whether there is enough testing of what people are doing and saying that they are doing. From your perspective as regulators, do you encourage red teaming? Do you have people testing these systems? Like we did in digital security at one stage with hacking, why do we not employ hackers, scammers and other people to find the weaknesses for us? Is that not much better than having lots of meetings in lots of different forums?

Mark Steward: I will try to answer that question. It is a good question. There is a good answer as well. The answer is, yes, of course we test. Where we see firms, certainly in the financial services sector, that have deficient systems and controls to prevent financial crime or to prevent money laundering, we take action. There have been a number of cases in recent months, starting most recently with the prosecution of NatWest

Bank for failing to have systems and controls in place to prevent money laundering. That was the first criminal prosecution of a bank for that offence in the UK. There has been a long history, and we can give you a list of those in writing, if you would like that.

Getting ahead of the fraudster is absolutely one of our priorities. One of the advantages we have with the increase in online scams and frauds in particular is that we have an opportunity to detect those scams when they first appear online. The old paradigm of fraud was that you only ever found out there had been fraud when the person who had been defrauded realised it themselves and made a complaint. It was invisible, which often meant the law enforcement process was starting long after the fraud had been perpetrated. That can be years in the case of investment scams and frauds. The deterioration of evidence and memory can be really difficult in those instances.

Online scamming, though, is different. It is happening in the moment; it is happening now. New sites are appearing every day. We surveil the internet on a daily basis to detect these sites. We identify them, and we publish their names on a warning list. That list is available to consumers, and we have public campaigns to market and advertise the utility of this list to people who are looking to invest to ensure they do not go near these sites. It is also available to banks and other payment services firms, which may be involved in processing payments to these sites as well.

The unique advantage we have with online scams is that we can often detect these things before anyone has been scammed. This is really important, and it needs to be made bigger; it needs to be magnified. We are doing as much as we possibly can, but we are only one unit in this picture. There are many other types of scams out there. At the moment we are seeing a reduction in the number of investment scams, but other scams are popping up that we do not have any statutory remit to look at, investigate or call out. This is an example of where the Online Safety Bill can have an enormous impact.

Q149 **Baroness Taylor of Bolton:** Earlier on, you said that fraudsters are "great innovators"; you have both said that. In a sense, you get the feeling that they are always one step ahead. What you have just been talking about, Mark, in the investment area does seem encouraging, though I am tempted to say, "If it is that good, why are so many people being scammed?" Maybe it is across the board in other sectors. There are lots of new types of scams. You mentioned delivery scams earlier. We are getting screen-sharing scams. The public is always a bit behind the curve in finding out about these, so a lot of things get through.

First of all, can you tell me what the most serious threats are? What are the new threats? You talked about red teaming in that particular area, but it is always a bit late. I did not know there was a daily issuing of information, but then I am not an investor. I know that I get scams on my phone and on the internet. There are lots of young people in particular who are becoming money mules and not understanding what is

out there in that respect. It is coming at people in so many different ways.

Although you might be red teaming and making some progress there, you also mentioned intelligence-sharing and the lack of investment and funding there. Is that a big area where we could make real significant change?

Chris Hemsley: There was a question there about the types of frauds. In terms of what I am seeing, particularly around payment fraud, which I am particularly focused on, traditional card fraud is starting to reduce. There have been some significant steps forward. Most recently, the FCA was working on the implementation of Strong Customer Authentication. It is the added layer of protection for online transactions in the card space.

Authorised fraud is the really big challenge. It is quite case-specific. The type of psychological manipulation that is used can vary, and it is quite difficult to get ahead of. We see that in a wide range of frauds. Investment fraud is in that space, but romance scams are another really difficult one to deal with. The classic impersonation fraud of pretending you are a bank, HMRC, the Post Office, a delivery firm or whatever is still very large in value and is still increasing. There is a real challenge there.

On your question about what to do about it, you rightly talk about information-sharing and making sure that everyone who can play a role does their part. There are two things that I would highlight in addition to that. One is that, from a payment system perspective, we know there are some gaps; we know there are some vulnerabilities in the system that we need to close.

The other aspect of this is that, while making sure, where we can, people are protected, we have to make sure the cost is felt in the right place. Ideally we would stop these frauds in the first place, but, if the cost is felt by people who can act, it creates a commercial incentive. We cannot just rely on the regulators to address this. We need payment firms; we need social media firms; we need everyone. If they feel a commercial pain from these frauds, it introduces a more commercial incentive. They are best placed to move quicker. That is the other point.

I am not disagreeing with any of the elements you have identified. We should try to use the commercial incentives by making sure the rules and the incentives are there for people to all play their part.

Baroness Taylor of Bolton: Are you saying that the gaps and vulnerabilities are not dealt with not because of a lack of ability to deal with them but because there is no real incentive? It is part of the business risk they take, and they write off certain things.

Chris Hemsley: I would not put it quite as black and white as that, because there are people who are doing the right thing and people who are stepping up. Equally, there are firms that are not doing enough today. The social media firms need to do more.

We have talked about the Online Safety Bill. Within the payments space at the moment, we have a voluntary system. It is great that the large retail banks have done the right thing by their customers and joined, but there are firms that have not. The firms that have not are not seeing the commercial cost, so they are not going to be doing as much. Some are trying to help and are doing the right thing, but we can go further.

Huw Saunders: There are a couple of points that I want to add, particularly around intelligence-sharing. This is not a UK-specific problem; this is a global problem. It is particularly felt in the Anglophone world to some degree, but, equally, it is targeting Chinese-speaking communities around the world as well.

The reality is that there is a great opportunity to learn from other jurisdictions. We speak on a regular basis with our counterparts in the US, Canada, Australia, last week Singapore and other places to understand what is going on and to see whether there is a threat there that is likely to be replicated in the UK.

I could cite an example from last year. You may have heard of a particularly malicious campaign called FluBot, which is a combination of so-called smishing—in other words, malicious texts—with an embedded website that downloads malware to your smartphone. That was flagged to us by our counterparts in Belgium. We were able to engage with operators in the UK and Google. This is specifically targeted at Android handsets. Google took measures to mitigate the impact of FluBot, which is still in place. That is an example of being proactive and looking at something before it really happens within the UK.

Equally, there are measures being taken, particularly within the telecom sector, to address that smishing problem, the problem of malicious texts. All four UK MNOs, mobile network operators, have implemented a machine learning or so-called artificial intelligence-based spam-shield service, which looks at the messages coming through and is very quick to spot patterns that are suspicious and block those messages getting to the end user. It is not perfect, but it can block over 90% of malicious texts. There is evidence that this has been highly effective at reducing this problem.

Equally, innovation will continue to happen. This is a continuing arms race, to some degree. At the moment, there is no evidence that the telcos are not prepared to continue to invest to try to be as proactive as possible.

Mark Steward: I just have one point that we have not responded to. Our ScamSmart campaigns are designed to provide consumers with up-to-date information on how scammers are operating, what techniques they use and what red flags exist that you can spot yourself to avoid being scammed. Huw mentioned Stop Scams UK. The banks also have variations of this. Citizens Watch has something as well.

There is information that should be available to consumers to get ahead of the game themselves as well. It is not a perfect answer, but it is really important that we have more self-aware and educated consumers to fight back against fraudsters as well. It cannot be done by law enforcement chasing scammers after the fact, nor can the regulatory system perfectly manage the entire ecosystem of fraud. We need to have consumer engagement here as well.

One issue, as we say in the written evidence that we provided, is that the campaigns that generate consumer awareness about how scams are operating are a little fragmented. There is no central government site that brings all of this together, which might concentrate and focus and ensure that there are no inconsistencies in those messages. Again, in order to keep that site relevant, you need to have up-to-date intelligence as to what scammers are doing. I really urge you to look at the ScamSmart website to get an idea of what information there is, what is available and how powerful, readable, simple and digestible it is for ordinary people, including me.

Q150 **The Chair:** Mark, you mentioned earlier on the list of alerts about websites. Does the FCA have the power to take down those websites, or do you have to rely on the internet domain companies?

Mark Steward: We work with partners, both here and overseas, to try to get the sites taken down. It can be hit and miss. Sometimes you can get them taken down, but, invariably, whoever is behind these sites just pops up with another one straightaway. It is a whack-a-mole game.

Again, that is why the Online Safety Bill is so important. It will allow Ofcom—we are happy to be involved as well—to introduce some KYC standards around how these sites get on the internet in the first place.

The Chair: You have set up our next phase of questioning brilliantly for Huw.

Q151 **Lord Allan of Hallam:** Yes, this is primarily a question for Huw and Ofcom. We are all expecting that at some point in 2023 you will gain the responsibility of regulating online platforms in respect of how they handle fraudulent advertising. The all-important details will be in codes of practice. We are very keen to hear from you any insights into the process and timetable for developing those codes of practice.

Huw Saunders: I am afraid I might unfortunately have to disappoint you there. I am not a specialist in the online safety sector at all. We are more than happy to answer any specific questions in this space. We will do so in writing after this event.

However, as you are aware, the legislative process is now underway. Indeed, a couple of my colleagues were giving evidence this week before the Bill Committee. The process overall is going to run for some time. As you say, we will be publishing codes of practice that will require the relevant players to do certain things to prevent harm happening. Economic harm is just one of the categories that is involved. This is a

large and complex area. We are spending an awful lot of time and effort and we are recruiting a hell of a lot of new resources to help us address this.

There is not much I can add in terms of detail at this stage, other than to say that we are extremely keen to get this underway, because we recognise the harms that are happening across the board a result of fraud. Economic harm is just part of the agenda, as I said. It fits into what we are doing already in the telco space to some degree. It is something we are very keen to work on, together with our other regulatory partners, in due course.

Lord Allan of Hallam: It would be very helpful, given the committee's subject matter, if you were able to share with us, having talked to colleagues, details of, in particular, the timetable and the process that will be used.

Huw Saunders: We will get back to you on that. If there is anything else that you would like to indicate to us, we would be more than happy to take those.

Lord Allan of Hallam: You are confident that you will have the resources.

Huw Saunders: Yes. As I say, we have been in discussion with the Government on this issue for some time. We have a programme for the recruitment of the appropriate people. We have opened a new facility in Manchester to enable us to have the physical space to have around 300 new colleagues, who will be specifically aimed at addressing online issues.

Q152 **Lord Browne of Ladyton:** We have been told—I am bound to say that the evidence we have heard from some of these quarters has encouraged us to believe this to be true—that telecom providers and tech platforms are not sufficiently incentivised, for whatever reason, to tackle fraud facilitated via their services. If you, for example, take these authorised push payment scams, particularly impersonation ones, they generally start off in the telecoms area with some text message or something.

My contract has free text messages, which I never use, and I do not know anybody else who uses them. It occurs to me that, if somebody is putting out 5,000 text messages a day, they are a fraudster. I do not know anybody else who does that.

The question is about how we can incentivise these sectors. Apart from the Online Safety Bill, as far as some of these platforms are concerned, what could be done to encourage these sectors to act more efficiently? It is the people who get into this ecosystem who hold the real key to this. It is the people who allow people into this ecosystem who hold the real key to this, is it not?

Huw Saunders: That is right, but I probably would take issue with the suggestion that the telecoms sector overall is not incentivised, because they actually are. The evidence of that is that they are prepared to invest

in solutions and platforms that are aimed at preventing malicious texts in particular from getting through. It is not a small amount of expenditure that is involved in doing this. They are investing all the time to prevent malicious messages from getting through. The difficulty is identifying them.

At the moment the reality is, as you have said, that there is a complex ecosystem out there. There are so many points of entry for malicious texts. By the time they get to the telco that faces the consumer, whether it is BT, Vodafone or whoever it might be, they have great difficulty in identifying whether this is likely to lead to harm. In terms of the SMS environment, as I have said, they have implemented systems that are trying to predict whether or not something is likely to be malicious. In the calls environment, that is next to impossible.

We are working with them to look at ways to prevent calls getting through that are obviously malicious. There is something called the "do not originate" list. Financial institutions, government agencies and others have nominated numbers that are commonly used for inbound calls but will not be used for outgoing calls. In the past, scammers have used that to say, "I'm from HMRC", "I'm from NatWest", or whatever. That is now a list of over 12,500 numbers, which, if they are seen in the network, are known to be malicious or known to be a scammer and therefore should be blocked. That has proven very effective. When this was introduced, HMRC saw the incidence of malicious HMRC impersonation fall by over 95% or something of that nature.

That is one example, but there are others. We have been working with the industry for a number of years to get them to introduce these things. They are very co-operative, but there is no silver bullet. In the longer term, we are working on something called CLI authentication, which gives you an assurance that the number being used is genuine and the person making the call has the right to use that number. That is going to take a couple of years to implement.

The package of measures we consulted on in the February documents we published are aimed at making sure industry knows what best practice looks like, so we can hold them to account. This is always going to be a process of encouraging them to do more. At the moment, as I say, they are incentivised. They bear the additional cost of having to invest in their networks to make them bigger than they should be just to carry that malicious traffic. It is not something that we think needs to be augmented with any further incentives at the moment.

Lord Browne of Ladyton: Maybe we could expand this slightly and move on to other tech platforms. I cannot see any reason, in this day and age, with the communications available, for people to be mass texting unless they are scammers, to be honest.

Huw Saunders: Just picking up on the text issue, there are, for a variety of reasons, a number of genuine business reasons why you want to send

texts out. The banks themselves use SMS significantly to communicate with their customers. Sometimes they are sent out in large volumes.

There are genuine reasons why this is allowable, but, on the other hand, I agree with you: an individual SIM card in an individual phone sending a large number of texts is suspicious. Indeed, all of the mobile network operators now put in place measures to identify whether they go over a particular volume and indeed block further texts coming from a particular SIM.

Q153 **Lord Sandhurst:** I would like to follow this up. I simply do not understand why there cannot be an obligation on them to know their advertiser, to know their customer. Why should there not be a duty to prevent fraud?

Huw Saunders: In terms of, in the UK, knowing who your consumers are, for instance, yes, I agree. It is part of the package of measures that I referred to already. When numbers are being used by businesses, we believe there is a due diligence process that needs to be gone through. We are giving greater guidance on what that should contain.

The reality is that this is a global network. There are entry points for calls and texts all around the world, which are far beyond our regulatory remit. Preventing those coming into the UK is a big challenge.

Lord Sandhurst: Can I press you on this? I accept it is probably difficult, but the fact is, if there was an obligation to prevent fraud, with financial consequences for telephone companies and others, they would take steps, would they not?

Huw Saunders: The point I am making is that they are taking steps already.

Lord Sandhurst: They are not effective, are they?

Huw Saunders: They are as effective as they can be with the current technology. Imposing an obligation to bear liability if they cannot prevent the calls or the SMSs getting through is not particularly equitable. If there is evidence that they are not doing things that we believe are necessary, we will seek to ensure they take the necessary steps.

Lord Sandhurst: We do not have time now, but would it be helpful to continue this in private? You or your colleagues could explain perhaps a bit more what some of the difficulties are.

Huw Saunders: I am more than happy to.

Q154 **Baroness Kingsmill:** All three of you have made some good points in relation to prevention. Recognising, as I do, how difficult it is, as a former regulator myself and a former director of a telco, I know perfectly well that change happens when there is a financial incentive to ensure that it happens. I wonder whether you had thought at all about a process by which victims of fraud could be compensated, a process of restitution. As

I said, prevention is the first line of defence, but, if it hurts the bottom line, it really makes a difference to the way in which companies operate.

The Chair: Are you particularly meaning the telecoms companies and the tech companies, rather than financial services companies?

Baroness Kingsmill: Financial services companies, as far as I can see, do not do a bad job of compensating their customers when they are the victims of fraud. The telcos need to make a bigger effort. I can think of ways in which it could happen, and I wondered whether you could.

Huw Saunders: In effect, this goes back to the point I have made already. We are working with the telcos, and have been for some time, to identify ways that they can prevent malicious messages getting through. At the moment, there is no evidence that the major players in the UK who are consumer-facing are failing to take this on board and work with us. As I said, if there were evidence that they are not adopting best practice or not implementing the appropriate solutions, I might have some sympathy with the position you are taking. At the moment, there is no evidence that is the case.

If you cannot identify that a message is malicious, and therefore you have no mechanism to prevent harm being felt by the target, it is quite difficult to justify, from a regulatory perspective, that you should bear the liability. The reality is that, yes, calls are made, texts are sent, emails are sent and doors are knocked on as a precursor to somebody being defrauded. One way or another, the common point, unfortunately, is the financial services industry. That is the bit that results in the loss of significant amounts of money. To ensure that there is some degree of liability, that is the area that has been rightly concentrated on to date.

In the telco sector, it is much more difficult. In any given call or any given text message, there may be five, six or even a dozen different telcos involved. Assigning liability in that context and preventing the message getting through in the first instance is extremely difficult. As I said, I am more than happy to talk about this in more detail offline.

The Chair: I have to say, Huw, you have been a far better advocate for the telecoms industry than the telecoms representatives were for themselves. We have a couple more of them coming before us, so perhaps they will take note of everything you have said and come with the details you have hinted at.

Q155 **Lord Sandhurst:** This is a question primarily aimed at Mark. The FCA regulates advertising for most financial services. We understand that last year Google, no doubt prodded by you, agreed to put in place a new verification policy to ensure that they only promoted authorised financial products. We also understand that in December Meta, Twitter and Microsoft said that they would do much the same.

I have three questions. Are they doing this? Is there a timeline? Secondly, more generally, how forthcoming is the tech sector? Thirdly, what could be done? What about a duty to prevent fraud?

Mark Steward: First, Google's change to its terms and conditions for paid-for advertising has been enormously helpful in reducing the scam ads that used to appear on searches for financial products. Since Google made the change, we have only spotted one ad that has snuck through; that is using the daily surveillance that we carry out.

Bing, which is Microsoft, has also adopted the same approach. We have seen similar success. Twitter has agreed to do so and is implementing it. We are testing now the extent to which that is in accordance with the expectations that we have. Meta has made noises, but they have not done it yet. We will lose patience with that process. We have seen a waterbed effect: there has been an increase in scams appearing on sites like Facebook and Instagram, sites that Meta operates.

It is hard to see what advantage they calculate exists for allowing this to continue. It really is very hard to see. If anything, it perhaps underscores some of the questions that have been asked here about whether there are incentives to do the right thing.

To come to your question about prevention, an offence of failing to prevent fraud is problematic. That is not because I come from a defensive posture for the industry; it is because of my law enforcement experience. It is a hard offence to prosecute. We should think long and hard about creating white elephant offences that look good and sound good but cannot be prosecuted.

By contrast, we have a regulatory regime in relation to financial services where there are regulatory rules and standards around preventing financial crime, monitoring transactions, knowing your customer, knowing your product and preventing money laundering. These are regulatory offences that carry with them the same unlimited fine that would probably exist for a criminal offence of failing to prevent fraud. In the financial services sector, these provisions work well; they are usable.

Lord Sandhurst: That was my point, really. The obligation might give rise to a criminal response in that sort of case, but, if you have the civil regulatory mechanism, it has just as good an effect, does it not? It is also easier to enforce, because they have to show they have taken reasonable steps.

Mark Steward: Having just prosecuted NatWest for its systems and controls in relation to money laundering, the existence of a criminal sanction for the most egregious cases is a good thing to have.

Lord Sandhurst: Yes, in your back pocket.

Mark Steward: Practically speaking, it is the regulatory environment that is really able to react far more ably and nimbly. The regulatory environment can also change the rules far more easily as well. A statutory offence needs Parliament to change it if it does not work. That can be a long process.

Lord Sandhurst: If the world wants to do this with, say, telcos or

advertisers, not the banks directly but with the platforms and so on, who would be the right regulator to look over that? Do we need to have several regulators?

Mark Steward: Where that responsibility would sit is ultimately a question for the Government, but the framework is a viable framework. It is implicit in the Online Safety Bill. That is what is being envisaged. Of course, the FCA is very happy to assist and work with Ofcom on this.

Lord Sandhurst: Would it be helpful to talk to you privately about the nuts and bolts and things?

Mark Steward: Yes, I am very happy to do that. I just want to make one further point about the changes in terms and conditions. It goes to something that is quite important about the tech sector and the way the tech giants operate. These are global businesses, and the initial reaction from the tech sector to a request to change terms and conditions to protect UK consumers was, "We can't make a change for the UK, because that would mean we've got to make a change for every other country as well. We are a global business".

There is an issue here about how the world really gets a grip on these global businesses. At the moment, there is no consensus across the world on how this is going to operate. We are going to continue to run into that problem with local solutions.

The Chair: It demonstrates why regulation, in the form of the Online Safety Bill, although it is UK-wide or UK-only, is a very valuable first step, as you have all said.

We need to check our evidence, but I am pretty sure—colleagues might remember—that on Monday we heard from Meta a firmer commitment to cracking down on fraudulent advertising than you have been able to give. We need to check the consistency, but I have a feeling that Meta may have over-promised. Mr Steward, thank you for giving us the timeline as far as the FCA is concerned. We will check that.

Q156 **Baroness Bowles of Berkhamsted:** Mark, the FCA reached an agreement with Google for up to $5 million advertisement credit and support to industry awareness campaigns. Have any other platforms stepped up to offer the same? I am also not sure what time period that goes over and how it measures up to the amount of money you were previously spending on the platform.

Mark Steward: So far Google is the only company that has made this offer to us. It is only Google at the moment. The credit that Google has offered to us is now in use. We previously spent our own money to pay for warnings and various other advertising to appear on Google's search pages when people were looking for investments to make. It is extremely helpful to be able to save valuable money, which we can spend on chasing the fraudsters, instead of paying it to Google.

We would like to continue that, but there is no offer to continue it beyond the credit that has been offered so far to us. As I say, no one else has offered that to us either.

Baroness Bowles of Berkhamsted: Would it be feasible to in some way make it mandatory? I am sure the answer would come back, "We can't do that just for the UK". One can legislate. They do want UK exposure.

Mark Steward: There is a lot to be said for public service advertising in this space to steer consumers away from potential scams and frauds. We have the ScamSmart website that I have mentioned. Others have other versions of that as well. It would be terrific if some of the messages that we have on that site were delivered in real time to consumers, as they are looking at things on the internet in particular.

Baroness Bowles of Berkhamsted: How feasible is that? Do we have the technology to do that?

Mark Steward: The technology is there to do that; it is the cost.

Baroness Bowles of Berkhamsted: You could make the platforms bear that cost.

Mark Steward: We cannot make them do it, no. We do not regulate them. We do not have that power. Do I think something like that would be effective if we could do more of it? Yes.

The Chair: Ofcom, this may not be something you can answer now, but perhaps that is something you might take away to colleagues and then write to us. You would be the obvious regulator, would you not?

Huw Saunders: Yes, it clearly would be more related to us in this context. I am more than happy to take that away.

Q157 **Lord Browne of Ladyton:** This question is directed to you, Mark. There is a question about whether the FCA has sufficient powers to take measures against financial services companies whose services or products are being used to perpetrate fraud.

It is interesting that twice you have made reference to the prosecution of NatWest, which was quite a significant prosecution. The money-laundering regulations under which they were persecuted were brought in 2007, which is 15 years ago. As far as I know, this is the one and only prosecution. I remember the case. It was about a Bradford jewellery business, which traded between 2006 and 2008. I might be wrong about those dates, but it was 2006 or 2008. It is hardly evidence that shows this is effective, if in 15 years there has been one prosecution, and that itself was pretty old. The interesting thing about it is that NatWest pleaded guilty when they got to court.

It seems to me to question whether or not there are sufficient powers. We create the framework within which you operate; I understand that. We have a shared responsibility for this, but do you have sufficient

powers?

Mark Steward: Yes, we do. That was the first criminal prosecution. Why is it the only prosecution? It is very difficult to prosecute a bank for a systems and controls offence and prove that beyond reasonable doubt. It is not straightforward; it is not simple. They pleaded guilty because we did a damn good job on the investigation, not because it was easy, simple or straightforward. It was a highly complex offence.

It is not the only example of the money-laundering regulations being enforced. I have promised you a list of various other cases that we have brought. That includes, over the last 12 months, dealing with systems and controls offences that are related to financial crime of one kind or another. The prosecution of the underlying transactions involving the Bradford jeweller commenced earlier this year; those were prosecutions brought by the police. It is an example of the way in which these cases are difficult to prosecute. It is an example of why a criminal offence is not the be-all and end-all. It is not the answer. Do we have sufficient powers? We will provide you with a list of cases that exist here.

In broad terms, the Financial Services and Markets Act—effectively, this is the legislation that the FCA administers, as well as things like the money laundering regs—creates a safe place for firms and investors to operate. Within that safe place, there are important rules and standards that need to be met. All those rules and standards are designed to ensure that safe place remains safe. If any of those rules are broken, there are consequences. There is an ombudsman scheme; there is a compensation scheme; there is the ability for the FCA to investigate, to enforce, to impose fines and to get redress for victims of those rule breaches.

Within that regulatory space, that safe space, with some exceptions—there are always going to be some exceptions where things go badly wrong—consumers are able to get good deals and fair outcomes. Outside that space is where fraud has proliferated. The online marketing of investment scams is all unregulated. It is outside the safe place that the regulatory system creates.

The objective of our public campaigns around ScamSmart is to try to persuade and convince people to operate within that safe regulated space and not be tempted by the glitter of online marketing campaigns. We need more of that. We just need more of it. We need to make sure that safe place remains safe. We need to do a better job at doing that as well, but we also need to encourage consumers that that is the case.

Lord Browne of Ladyton: That is a very interesting and very broad answer to the question I asked. In the story of a scam, the money is laundered somewhere, usually. Quite often, at least in this country, it is laundered by businesses that you regulate. Let us take cryptocurrency, for example. The money laundering legislation does not only apply to banks. It applies to people who sell crypto-assets. You regulate that. I would not be able to sell these if I was not registered with you.

A very small number of businesses are registered with you, and you helpfully produce a list of the people who are not, who you believe are conducting business. You have the power to shut them down, so why are they on a list? As far as I am concerned, this list has two functions. It warns me if I do not want to trade with scammers, but, if I am a money launderer, it also tells me where I can go to find people who are not compliant with money laundering legislation, if I want to use cryptocurrency. It is double-edged.

I would prefer that they were shut down. Why are they not shut down? You believe they are operating and you have the power to stop them. Why is that happening?

Mark Steward: Many of them do not have a legitimate address, for a start. Most of them have closed down since we published their names. We can provide you with some information about that. Publishing their names and telling people, "These are businesses that are not meant to be carrying out this business, because they have not been registered with the FCA", is an enormously powerful disincentive not only for consumers to use them but for criminals as well. It is a big red flag for criminals as well. Criminals do not go near these businesses, because they have been identified and spotted. It is a very powerful, simple and cheap technique that does in fact close them down.

Lord Browne of Ladyton: I would love to see the data that informs that conclusion.

The Chair: If it is something you can share with us, that would be helpful.

Q158 **Lord Young of Cookham:** Can we go back to authorised push payments? Chris, you mentioned earlier on that you were getting more data on them. I have a number of questions on this. First, at the moment it is the payer's bank who is in the frame for compensation if things go wrong. Is there a case for looking at the payee's bank? It is the payee's bank that has allowed the fraudster to set up a bank account and launder the money through it. Do you have a view on putting more onus on the payee's bank, rather than exclusively on the payer's bank, when it comes to compensation or indeed regulatory action?

Chris Hemsley: The straight answer to that is, "Yes, we should". This is something that I have said previously. To unpack that a little bit, we have rolled out the voluntary code that offers that protection. The people who have signed up have particularly been the sending firms, and the sending firms have accepted liability.

That is the first step. We then need to move to a more sophisticated system over the time. One of the next steps we need to take is to make sure all firms participate. This issue of mandatory involvement is really important. We need to get the receiving firms in the system. When we have that mandatory involvement, exactly as you said, it allows us to share the liability between the sender and receiver.

Over time, I would like to do that in a smarter and more sophisticated way. For certain types of fraud, you could probably make the case that it is the receiving bank that should carry the bulk of the liability. Take a purchase, for example. Typically what you see in card schemes is that most of the liability is on the receiving side. For a peer-to-peer transaction between two private individuals, the current system might be broadly right. It is the sending bank that needs to confirm that it is going where it is meant to.

To go back to my straighter answer, yes, I agree with you that we need to get that balance better.

Lord Young of Cookham: Another issue that has been raised with us is whether there should be a delay before the payment goes through in real time. Some witnesses have made the case for there being a delay to give the victim, or the victim's bank, time to stop the transaction going through. Others have suggested that there should be a threshold to which the delay would apply. Another witness was against that but said that there should be more detection upstream to identify which transactions were likely to be fraudulent. Do you have a view on the issue of delay and, related to that, the issue of more identification of potentially fraudulent transactions before they take place?

Chris Hemsley: Yes. On the debate around delaying payments, one of the really important distinctions that might explain some of the difference of views is whether we are talking about the capability of the payments system or the speed with which payments are instructed into it. For the payment system, in terms of the core technical capability, the UK needs a faster, more secure, higher-capacity payment system. Slowing down that central system is likely not the answer, but we need to get smarter about how we introduce payments into it.

This is an area that we need to explore, and we can hopefully move forward and think of a better way of doing it as we get the incentives sharper here. I agree that there is something in here around the fact that, if I go on to my internet banking today and send a few pounds to buy something small, send some money to a friend or put down a house deposit of a five-figure sum or more, the experience is pretty much the same.

We are moving. Banks are starting to get that experience a bit different, but it still looks and feels pretty much the same, whereas there is something in this. Most customers would agree that, if I am using my bank account to pay for something like a coffee, it needs to go through quickly. If I am moving potentially life-changing sums of money, a delay of what might be five minutes is not a return to the bad old days of five days to clear funds. It buys a bit of time for the prevention mechanisms to kick in.

Lord Young of Cookham: There is some calibration. My final question on this one is the question of moral hazard. If you are overgenerous in compensating the customer, does that not reduce the incentive on the

customer to take sensible precautions? Where do you draw the line?

Chris Hemsley: We need to make two steps. One is to make these minimum standards of behaviour part of the system. They are just rules. Everyone participates. We then need to get better at what those rules are. We have all been talking about this sense that all parties need to play their part, and so it means that customers have a role in being informed and taking some care. Clearly, payment firms need to show responsibility, as do those outside.

We need to be a bit more refined in how we deal with this issue of moral hazard. Not all frauds are the same. Certain types of fraud are lower-value and repeat. If I am buying something on the street with some cash, I know no protections are available. You adapt and learn from that experience. You know that, if you lose some money in cash, it is gone.

In the digital space, for certain types of fraud, there is a good debate to be had about whether being protected once, twice or three times on a purchase scam is the extent of the protection. I would distinguish that from some of the worst types of these frauds. We are talking about people who have lost their life savings. On that, the moral hazard argument does not really weigh very heavily. I have fallen for this. When you are transferring large sums, you try to take care. Those who are transferring large sums and are defrauded may have been vulnerable or responding to quite sophisticated frauds and criminals who knew about psychology and how to manipulate people. If you lose your life savings, it does not matter that you have learned because it is gone.

The point that I am trying to make is that the solution between low-value purchases, for example, and the solution for these life-changing amounts is different, and the moral hazard argument weighs quite differently.

Lord Young of Cookham: We touched on GDPR and data a little earlier on in response to Baroness Henig. Are there any problems about banks sharing data? Do the issues of privacy prevent banks tipping off other banks that, "This customer is one that we have closed the account for, and we think you ought to know that, if he comes to you, you ought to be very careful before you open an account for him, her or the business"?

Chris Hemsley: If I make a start on that, I talked a bit earlier about when we were rolling out the name-checking service and confirmation of pay and that we worked with the Information Commissioner's Office to make sure that worked. We also have work under way now to improve the sharing of information between payment firms and introduce working with Pay.UK. We are chairing a co-ordination steering group to make sure that is happening. Later this year, the technology should start to improve and be rolled out so that payment firms that are receiving money can share more information with those that are sending it, and vice versa.

It is a bit similar to the example that you talked about. Some of that information is not personal information. It is not the sort of information that data protection or GDPR is trying to prevent from being shared. It

can be relatively simple information such as how long an account has been open. If the account has been open for days rather than years, it starts to help the sending bank to understand and risk-rate that transaction and know whether it should send it through.

That is the next step in what industry can do in terms of sharing information. What are the high-value bits of information that you can share? Of course, due diligence is needed to make sure that we are complying with all the relevant rules, but we can go for quite a lot before we start tripping over those—

Lord Young of Cookham: In a nutshell, GDPR is not an issue.

Chris Hemsley: It is not the thing that is going to stop us making progress. There is some low-hanging fruit that we can go for to improve information-sharing before we get anywhere close to the GDPR being the principal issue.

Huw Saunders: The one point I was going to make is that it is not just within a sector; it is cross-sector as well. The point I made earlier is that there some examples of where sharing information between the financial services sector and telcos in this context is worthwhile. We would encourage that where appropriate. On the same point, I do not necessarily regard GDPR as preventing this in any real sense at the moment, but the ICO will need to give guidance on it on a case-by-case basis.

Q159 **The Chair:** I want to ask each of you the final question in a moment, which is just what your one recommendation for Government would be. At the beginning, each of you talked about working together, but there are gaps. I wonder whether there are any gaps that we have not picked up on as a committee—we have probed into various areas—or if there is anything that we have not talked about.

In the FCA's written evidence, you talked about working with the PSR and running a TechSprint on APP fraud focusing on suspicious social media and scam promotions. We are all curious about what a TechSprint is and whether those are a couple of the gaps that you have identified in working together.

Mark Steward: I will start with the TechSprint. It is a voguish word that people tend to use for a group of people coming together to learn about something that they have in common. We did one last week on crypto. It was us, as the regulator, trying to understand more about how the crypto industry operates from people in the industry because it is developing so quickly.

On the APP one, there are people in both PSR and the FCA who are engaged in work on this. It is an opportunity for us to formally get together, swap notes and work out ways in which we can collaborate better in the future. There is no magic in the name "TechSprint".

The Chair: Are there any gaps that we have not identified in questioning

this morning? We might not have time to go into them, but it would be helpful to know. Also, if you each had one recommendation for the Government and the most important thing that you would like us to take away from your evidence on this subject, that would be very helpful to hear.

Mark Steward: The biggest gap is the one that we have discussed, which is in relation to online regulation or the absence of online regulation. I hesitate to say one thing because our written evidence contains more than one thing. If I were to choose one thing—I am loath to—it would be funding for the NECC and the police. There needs to be a sea change in the pursuit of fraudsters. We have talked a lot about prevention, and prevention is really important, but we have not talked a lot about pursuit; pursuit is really important as well. There should be no green light for fraudsters, and we are in danger of sending a green light. It is funding, purely and simply, and also funding for the NECC.

Chris Hemsley: We have covered the gaps. Most recently, that conversation around the receiving institution was a really important one.

The thing that we have been pushing for that makes a real difference for us is allowing us to use our powers fully. The issue is that this legislation currently prevents us from using our powers of direction to directly get at these issues by changing rules and placing requirements on firms.

The good news is that Government have been supportive of that and accept the argument, and it was included in the Queen's Speech in terms of the legislative programme. That is the key thing. It will allow us to move from a system in which we are reliant on firms to do the right thing. It is great that some have, but we really need these to be minimum standards. We need the powers to move it so that it is a minimum standard and we can then make sure that protection and the prevention piece are backed by the full weight of our powers.

Huw Saunders: The obvious gap is the one that Mark has addressed already in terms of online. Clearly, we will be heavily involved in this going forward.

In terms of recommendations, "no one easy answer" is the way that I would position us on this. The three areas that we have touched on many times already are probably the most obvious for any potential candidates. One is about improving information for consumers so that they can identify when they are potentially being scammed. The other is promoting and facilitating the sort of cross-collaboration that we have spoken about already, not just between regulators, but also with sectors. Finally, it eventually might be appropriate to introduce new measures to ensure the implementation of the appropriate technical solutions. At the moment, there is no particular measure that we can identify that really needs to be pursued.

The Chair: Thank you all very much indeed for your time this morning. Despite the fact that some people love appearing in front of select

committees, they still take time to prepare for, so we are really grateful to you for your time. There are a few areas in which we might follow up in writing, so thank you for that.