Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 23 June 2022

9.30 am

Watch the meeting

Members present: Lord Browne of Ladyton (In the Chair); Lord Allan of Hallam; Baroness Bowles of Berkhamsted; Viscount Colville of Culross; Lord Gilbert of Panteg; Baroness Henig; Baroness Kingsmill; Lord Sandhurst; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 22 Heard in Public Questions 231 - 240

Witnesses

I: Adrian Gorham, Chair, Communications Crime Strategy Group; Professor Feng Hao, Professor of Security Engineering, University of Warwick.

Examination of witnesses

Adrian Gorham and Professor Feng Hao.

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's website. You will have the opportunity to make corrections to that transcript where necessary.

I am very grateful to our witnesses this morning: Adrian Gorham, chair of the Communications Crime Strategy Group, and Professor Feng Hao, Professor of Security Engineering at the University of Warwick. Welcome, gentlemen, and thank you both very much for joining us. Time is short, so without further ado I ask Baroness Henig to put the first question.

Q231 **Baroness Henig:** Good morning to both of our witnesses. By way of an introductory question, what key trends do you observe in the ways in which telecoms services are being used to facilitate fraud today?

Adrian Gorham: Good morning to all the members of the committee. Thank you for giving me the opportunity to come along today, even though it is virtual.

Statistics from the Office for National Statistics show that, while most types of crime have declined since the mid-1990s, fraud and computer misuse have been growing. Reasons for the increase in fraud using communications services are exploitation by fraudsters as a result of two things. First, global technology has developed very quickly. We have had digitalisation. We have had the development of fibre networks, which give people more connectivity in the home and more speed. We have also had the rollout of 5G and 4G networks and smartphones, et cetera, which are more powerful. Those, and applications such as WhatsApp, are one of the reasons why there is much more exploitation.

Secondly, the actual price of making calls and sending messages on the networks is a lot cheaper. This was a public policy choice that has driven prices down through regulation. It has reduced the price of calls and SMSs to the benefit of customers. The unintended consequence, however, is that it is very cheap for fraudsters to try to contact their victims in this new world.

There are probably six or seven different ways that are utilised by fraudsters to try to reach victims. It can be a voice call; they call the person. It can be an SMS—the old text message that somebody receives. It can be an email, or an instant message like WhatsApp. They do it through an online platform or a combination of approaches that allow them to reach the individuals they are ultimately looking to defraud.

Some of the recent trends we see at industry level are certainly scam calls. I am sure that we all receive scam calls. I receive scam calls, be it at home or on my mobile. The second thing is the one-ring call, where you get a call from a missed number that you do not recognise. It is an international number, and if you call that number it is charged at a very high rate. That is another challenge we have.

There are also unsolicited SMS scams, when you get a text message that purports to be from DHL, the Post Office or whoever. Of course, they send out messages too. There is still an issue with SIM swaps, but that is very much disappearing these days.

Finally, for us, there is subscription fraud, which is by far the biggest loss to the industry. A subscription fraud is where the fraudsters purport to be a legitimate customer, or steal somebody’s identity, and they do it because they want to get themselves a mobile device. Mobile devices can range from £500 to £1,000-plus, so they are actually committing a fraud to obtain very valuable property. That is my opening comment on that question.

Baroness Henig: Thank you. Professor Hao?

Professor Feng Hao: First, I thank the members of the committee for giving me the opportunity to present oral evidence. Adrian has given a good overall picture of the trends. I want to add two points from the academic or research perspective.

In the telecommunications system, we have witnessed two trends. One is increasing social engineering attacks against end-users through telecommunication systems. This is enabled by two factors. One is automation. Traditionally, a phone call is made by a human; it is a manual process. Now, with computers, you can make a computer dial the phone number, so you can dial calls at very large volume and effectively spam lots of people in a very short time. That is done because of the technology; spammers can do it by a computer.

The second factor is spoofing, which is becoming an increasingly serious problem. When you receive a phone call, the number displayed on the phone is not trustworthy. It could be an arbitrary number. That is part of the social engineering attack. Criminals use it a lot, frequently to trick end-users that they are calling from banks, HMRC and other trusted associations, but actually the number is spoofed. That is a social engineering attack. Of course, as part of the social engineering attack criminals make use of SMS. They can also spoof the sender of the SMS. An SMS message could come from an arbitrary sender identity, but you cannot check it. Sometimes an SMS has an embedded URL for a user to click directly on to a website.

The second trend we have seen is that because the telephone system has inherent flaws, it provides opportunities for attackers to make a more sophisticated attack. One example is the SIM swap attack mentioned by Adrian. The users are totally unaware. They have a phone number, but the criminals get a new SIM card and somehow use social engineering attacks to convince the operator at the telecom company to transfer the number to a new SIM card, so they have total control of your SMS messages and phone calls. That can be very devastating for the end-user if they use SMS as the only recovery mechanism for their Twitter account or bank account. Once you lose control of your phone number, you lose control of your email and other things. That can be quite an effective attack. At the moment, it is a bit complicated for the attacker to perform this kind of attack, so usually it is a targeted attack and not on a bigger scale.

Another thing is an SS7 attack. We have legacy systems based on mobile and landline phones, using the SS7 protocols, but they have inherent vulnerabilities. If the criminals have somehow got corporate access to the SS7 network, they can do lots of things; for example, they can intercept your phone calls and SMS messages. They can also track the movement of people, how you hold the phone and move to different places. It requires special access to the SS7 network. It is possible, but it is not scalable because it is expensive. Usually, criminals use this kind of attack to target certain individuals such as high-profile celebrities or politicians, but not on a larger scale. Those are the two trends I wanted to cover.

Baroness Henig: Thank you very much for that. I think that sets the scene for what we do about all this.

The Chair: I want to drill down a little into the last part of your evidence, Professor Hao. You said that somehow they have access to the SS7 network. Can you expand on the somehow, and while you are at it can you expand on the mechanism that is used to trick one network into accepting a customer who belongs to another network? How does that actually happen? You say that it is social engineering, but what is the social engineering?

Professor Feng Hao: There are global SS7 networks, and all these networks need to interconnect. They need to work together as one system, but they are distributed in different countries. Usually, the system is closed to criminals, but certain companies can have special corporate access to the system. If they have privileged access to the system, they essentially become an insider of the SS7 system. The design of the SS7 system is that everyone inside the system is trusted with their behaviour, but because the system has grown so big and global it is difficult to enforce that every corporate access to the system is always honest.

The Chair: Thank you. Adrian, do you want to engage with that last question?

Adrian Gorham: I am not a technical expert and I would never pronounce to be. I think that is a very minimal risk in the UK. There are many types of frauds and things that can happen, but that one and intercepting calls are not on any scale. It is very minor.

These are international standards. We run networks using GSM, which is the global authority where all the operators come together to set all the standards for security, fraud and everything. They are all international standards and are not just relevant to the UK. We run a global phone network, and we are using global standards. They are not standards that just work within the UK.

Q232 **Lord Allan of Hallam:** Professor Hao, I want to dig into something else you raised, which is number spoofing. We have heard evidence of how effective that is as a mechanism for fraud, because people believe the call is coming from a trusted source. I am curious to understand what you see as the trend. Is number spoofing getting easier or harder over time? What has to happen to prevent number spoofing?

Professor Feng Hao: Thank you, Lord Allan, for this question. The trend in spoofing is that it is getting easier, and more prevalent. First, number spoofing is always possible. From the day the telephone system was designed you could modify the caller ID. To use the analogy of posting a letter, a telephone is just a way of communication. You can think of it as posting a letter. You write the receiver’s address, and you can also write the sender’s address on the envelope. You can arbitrarily write a sender’s address. It is your choice. Sometimes, if you post a letter from home, for example, you may want to write a different sender's address because you want the receiver to return the letter to a different address, maybe to your work address.

The telephone system works on a similar idea. When you make a phone call, the system automatically attaches your current phone number as the caller ID, and that is displayed on the receiver's phone so that the receiver can call you back. As a feature of the system, it allows you to change the phone number. There are legitimate reasons why you might want to do that. For example, you might want the receiver to return-call to a different phone number, to your mobile phone number. Or maybe you do not want your residential phone number to be displayed on the receiver's side; you want the receiver to call back to your work number. There are legitimate reasons why you might want to modify the caller ID.

The problem is misuse of that feature. In the traditional system, you need special hardware or special access to the network in order to modify caller ID. Now, as the system grows, and because of the deregulation of the market, more and more telecommunication companies use voice over IP-based technology. With those kinds of companies the service is in the cloud, so it is much easier to modify a number. It provides a very easy interface for a user to modify the number. It could be an app on your phone or a web page on your browser. You just need to specify what number you want to display. That number will be sent out to the receiver, and because of the way the telecommunication system is designed the number is only checked by the initial subscriber's network. If they do not block it, it will go through. For all subsequent networks, it is not checked because it is not possible for them to check. Modifying the number is always possible, but because of voice over IP it becomes so trivial that anyone can modify it.

Lord Allan of Hallam: Thank you. That is depressing. Adrian, I am curious about the response from the operators' point of view. We understand that Ofcom, for example, has issued guidance that was implemented by TalkTalk. To use Professor Hao's analogy, in essence if a letter has been sent from abroad but has a UK address on the back, we can assume it is untrustworthy. We are curious about measures like that and what the industry is doing to implement tools that can say, "This is likely to be a spoof number", and therefore stop the call at the destination.

Adrian Gorham: Spoofing is a very topical question. Yes, a lot of this is overseas. It is a global network, and when we receive a call we go by what the call says. I am sure we all appreciate how many tens of millions of calls there are every day. We cannot look at each call.

There is an initiative at the moment with Ofcom and the operators in the UK looking at this very issue, what the options are and how we can deal with it by using technology. I believe—I might be wrong—that it is due to report at the end of the summer. I am not sure whether you have spoken to Ofcom, but certainly members of all the operators are part of that group. You referred to an initiative by TalkTalk. There are different initiatives out there, which we are looking at to see which is the best one. I doubt there will be a silver bullet on this, but we are looking at them.

One other thing that we do in the UK for the banks is that we have a facility where you cannot spoof certain numbers. We reject them. It is called "Do Not Originate". For some of the banks, on the back of your banking card, the network bars you from using those numbers as a CLI, because you can imagine the impact it can have. So, tactically, our response to spoofing has been to use Ofcom's Do Not Originate list of banks'/financial institutions' main phone numbers for their in-bound calls to identify and block calls using these numbers as CLI. Hence, "spoofing" of banks'/financial institutions' main phone numbers has become more difficult, not easier. But there is a much bigger issue. We are working on that with the regulator and globally with the industry.

Lord Allan of Hallam: That is very helpful. We look forward to seeing the work from Ofcom. On the back of that, and slightly tangentially, a lot of people do not spoof; they use real phone numbers. The classic reaction for a lot of us is that we do a reverse number look-up. There are some really useful services that give you people's feedback on whether they are scam calls. I was curious to look at them. Should I Answer is a Czech company. Whocalledme.co.uk is a Polish company. They look like small entrepreneurs who are building these sites and then getting ad revenue from them. There does not seem to be an official telecom industry "Who called me" site. I am curious as to why that does not exist, because I think a lot of people would find it useful.

Adrian Gorham: I do not know. I can take that away and look at it. The other challenges in this world are things like number portability. In the good old days, you had a number and it was fixed with an operator. If you moved to another operator, you took out a new number. Number portability was brought in a number of years ago, but there is no central register. Each operator just passes the call on to somebody else. As networks have expanded, and more operators have come in, with more competition, it has just made that a more complex subject for people.

Lord Allan of Hallam: Thank you very much. It would be helpful if you could get back to us on the specific question of whether the industry has looked at doing a "Who called me" service, and your view is on the usefulness of that.

Q233 **Lord Vaux of Harrowden:** Adrian Gorham, you talked about receiving scam calls and texts, as we all do regularly. We have heard how these often originate through SIM farms, which allow bulk scam calls and SMSs to be made.

First, could you explain a bit about how the scammers are able to get hold of the equipment, in particular the bulk SIM cards and phone numbers that they seem to be using to make scam calls and SMSs? Secondly, in written evidence, the CCSG emphasised the need for realism about what can be done about this. Perhaps you could explain what realistically can be done, and what is being done.

Adrian Gorham: Scam calls and SMSs have actually been identified as priorities under the fraud charter that we signed up to with the Home Office. They are under actions 1 and 2, so they are areas that we are actively moving forward on. We have a range of techniques in place, including filtering and blocking, to try to identify and prevent those sorts of fraud vectors from reaching our customers.

SIM farms are an example of a technology development that facilitates the sending of automated SMSs in bulk, however, bulk SMS origination was already an issue with mobile devices and PCs. We are not aware of SIM farms actually generating scam calls. They are purely for sending bulk text messages. This reflects the different nature of the frauds involved.

Different mobile providers have different strategies and technical measures to try to suppress the bulk SMS messages coming from SIM farms.

The types of things that they include are limits on the number of SMSs that can be sent from a newly connected SIM card; we may say that it can only send 50 messages in the first week. There are technology enhancements to reduce the time taken to bar those services from SIM cards. We are trying to speed up the processes for barring. We are also looking at SMS filters that could actually conduct real-time analysis of the SMS messages, the patterns, and try to block them.

With the introduction of SMS filtering, providers look at the content of an SMS before delivery. Where providers identify content as a scam, we will block this from being delivered to a customer.

These solutions are designed to limit the businesses of the fraudsters sending bulk scam messages on our networks and internationally.

To give greater protection, one of the things that was recently launched and has been very successful is the 7726 service, getting our customers to forward any suspicious message to 7726, where it can be looked at and we can put blocks in place on the network. Does that answer that?

Lord Vaux of Harrowden: It does to a large extent. In order to make all these calls, scammers are getting hold of large numbers of SIM cards and phone numbers. Where do they get them from? How do they acquire them?

Adrian Gorham: These are purchased in person or on-line. The UK has encouraged an extensive competitive market in SIM-only services and these allow the purchase of SIM cards for personal and corporate use. There are multiple providers globally who provide SIM cards.

Lord Vaux of Harrowden: But the issue is the bulk. Anyone can go and get a SIM card, but why would anyone be buying 100 or whatever it is? Is that an area we can look at?

Adrian Gorham: You can go to the local corner shop and say, "I'd like to buy 10 SIM cards". They might be £10 each and have unlimited calls. They will sell you the 10. There is no limit and no credit checking. Many years ago, we opened up communications to all sectors of life and credit checks went. That is why they brought in prepaid cards and why the industry had to bring them in: so we do not have all the checks and balances in place that you would normally have.

My colleague would probably be best to comment on the type of equipment they use to make these calls. I am sure it is computers and everything, but I am not a technical expert to comment on that.

Lord Vaux of Harrowden: I think we are coming on to KYC issues and things like that, so I will leave that for later.

You mentioned the 7726 situation. My understanding is that although it is there and it works, very few people are aware of it. In the last two years, 12,000 scams have been removed, but that is a very small number. How do you make it more effective?

Adrian Gorham: I actually reported something to it this morning, because somebody had just tried to commit a fraud on me with Royal Mail. I know that will go to the operators, who will see it and share the information with the NCSC, and the process is there in the background. The more publicity we do around that, the better.

Outside that service, for all consumers in the UK, social engineering is a problem across many vectors. The more we can do centrally for customers' awareness of these kinds of scams, the better. They go across many areas. It can be your pension. There are so many areas where it happens these days. I am a big advocate of doing more centrally to make our citizens more cyber-savvy, in a way, to help protect them.

Lord Vaux of Harrowden: Professor Hao, do you want to comment on that, and explain any more about how SIM farms and bulk numbers are used by the scammers? That would be helpful.

Professor Feng Hao: Before this hearing, I had a chance to talk with some telcos. Different groups in different countries may operate slightly differently, but it is basically a piece of hardware that you can buy online in different countries and it is very easy to get. You need a SIM card. For the criminals it is a distributed network. Because of different payment schemes for the SIM cards, they tend to buy the prepayment SIM card. That kind of SIM card is usually quite cheap; for example, for £150 you can buy thousands. It will depend on the kind of scheme it is. They put thousands of these SIM cards into the SIM farm and they can send SMS messages.

For the prepayment scheme they sometimes provide an unlimited SMS service. Of course, there are terms and conditions, but the criminals just ignore the terms and conditions and send SMSs in bulk. There is a detection mechanism, so they can be detected by the telecom company.

It takes time, but once it is detected they can shut it down and block the numbers. But the loss for the criminals is only £150, so they just buy other SIM cards. It is cat and mouse, because there is no identity check, and sometimes they use false identities to buy things. So once the number is blocked, they simply move on to new numbers. That is the problem. This kind of attack is difficult to block.

Lord Vaux of Harrowden: Do most of them come from overseas or from this country? Is there a differentiation that would allow us to block bulk overseas SMS calls, or something like that?

Professor Feng Hao: For a lot of SMS messages, whether from the UK or overseas, I think Adrian might be the best person to answer. There are markets to buy SIM cards very easily. I do not expect there is any difficulty in buying SIM cards in the UK. Once you have a group of people and they are all distributed, you can buy a lot of SIM cards. It is very difficult to check. Even if the telecom company can detect that the SIM cards have been abused and stop it, the criminals can simply buy new SIM cards.

Adrian Gorham: To build on that, this is a global problem. We are globally connected in the UK. Very often, the messages, calls and texts that people receive come from overseas. Often, when you get social engineering phone calls, the person is not sitting somewhere in the UK. They are sitting somewhere else in the world and you are one of many calls they are making that day, trying to trick you into doing something.

Lord Vaux of Harrowden: Is there a solution in identifying bulk overseas calls? Is that part of the screening you are doing?

Adrian Gorham: That is part of the screening that we are doing. It is not easy, but we are trying to identify where we have numbers and evidence that it is fraudulent. We would look to bar those numbers, take down the service or, if we have a link to a website, we bar it on our networks. That is all the work we are doing behind the 7726 service, but it is not a silver bullet. Fraudsters develop their methods all the time.

Lord Vaux of Harrowden: Thank you. I am sure we could talk about this for hours.

Lord Sandhurst: I had never heard of 7726, and we have heard a lot of evidence. It is obviously a good idea. You said that it gets publicity, but should there not be mainstream advertising of it to everyone? When you get your phone, should there be a big red notice put in it, and possibly something even on the television, on Netflix and everywhere else?

Adrian Gorham: Certainly NCSC is very public about the use of the service and that it should be used by people. We as operators do. It is on our website and everything that we do. I can certainly look again at whether there are broader comms channels where it would be beneficial to share that information. Most of it is in the digital forms, as we stand.

Q234 **Lord Young of Cookham:** Can we turn to the incentives which the telecoms sector has to clamp down on fraud? On the one hand, clearly the more calls that are made, the more revenue the telecoms sector gets. On the other hand, we have heard about loss of brand image, subscriber churn and the rest. Have we got the balance right? Should the telecoms sector be incentivised more to act on scams? Should there be tougher action by the sector on those who perpetrate them?

Adrian Gorham: In our written evidence that I think came in a few weeks ago, we made the point that the financial model of the communications sector is no longer the historical one, where we charged for inbound SMS or call revenues; they are not a significant revenue stream. These days, people have big bundles combining all their calls, SMS and data, and that is now the norm. The growth of the internet and the introduction of competition and price controls by regulators mean that communications sector revenue is dominated by its retail revenue. The revenue of our members is what they charge for their service bundle, and that is what drives our overall commercial success. No formal assessment of the cost of fraud has been done by the industry. Things like the service cost of handling complaints and the reputational costs of dealing with fraud can easily exceed the revenue that we would get from the actual calls or the text messages.

Regarding further action by the sector, to clarify what we said before, we are focusing on what we can do to prevent these types of fraud. At the back end of last year, we launched the fraud charter, for which we agreed all our priorities with the Home Office and its consultants. It was based on the most urgent issues and where we could make the biggest impact to protect customers, and then looking at where new frauds can emerge. I do not think there is an incentive there. These are often our customers, and we want to do what we can to protect them, so we are all joined up in that.

Lord Young of Cookham: You said a few moments ago that you had been the victim of a scam and you reported it to the NCSC. In addition to all the work that is done on barring, blocking bulk voice calls, restricting use of calling time and restricting financial return, should you be doing more to actually catch the fraudsters—in other words, not just stopping them but providing the necessary evidence for the prosecution authorities and the police to actually get them—so that it is not a nil-risk operation at all, and the risk of getting caught is higher than it is at the moment.

Adrian Gorham: That is a great question. I have mentioned one of my key messages already, which is about the public’s awareness of scams in general. The second concerns the actual enforcement of the law. Crime pays. We need to do a lot more with law enforcement, and we need to make sure that law enforcement and the other agencies are resourced and structured to be more effective in acting against this serious and repeated fraud against our customers. The resources for law enforcement and the agencies should properly reflect the impact this is having on the economy and on crime in the UK. I very much feel that one of the key ways of tackling the issue is to catch some people and bring them before the courts.

Lord Young of Cookham: Professor Hao, I appreciate that this is not your prime interest in the sector, but do you have any footnotes on what we have heard from Mr Gorham?

Professor Feng Hao: I want to add some remarks about incentives. Typically, scamming attacks involve the banks and the telecommunication companies, so we can compare the two. In the banking sector, the PSR—the Payment Systems Regulator—has a bank code to encourage large banks to reimburse victims. It is a very good initiative; it is in the right direction and gives the right incentive for the banks to compensate the victims. It also tightens their security.

In the telecommunications system at the moment, when someone receives a spoofed phone call claiming to be from a bank or HMRC and is tricked into making a payment, the telecommunication companies are not liable. There is also a lack of incentive for the telecom companies to address these problems aggressively, partly because the telcos are driven by revenues. To stop these kinds of attacks, they need to invest, and that does not bring in additional revenue, so there is a misalignment of incentives.

Lord Young of Cookham: That is a very interesting remark. My colleague Baroness Bowles will, I think, pursue this downstream.

Q235 **Viscount Colville of Culross:** Good morning. The committee has heard evidence about the importance of know your customer and know your business customer checks. Ofcom recently issued a new set of guidelines that expect phone companies to run know your customer checks on business customers by checking them with a range of agencies to uncover any indication of high risk of possible mobile phone fraud. Is that enough, or does the guidance need to be mandated or even extended?

Professor Feng Hao: Checking the identity of a customer or business customer is crucial, but there are some fundamental limitations to how far you can do that. In the case of the telephone system, Ofcom is the wholesaler; it has a block of telephone numbers. It does wholesale to a few companies, and it can check the identity of a company and its business identity. That is all fine. Then there is the retail level, where each company retails numbers to retailers, and each retailer will retail their numbers to sub-retailers, so there is a very high chain, all the way down to the end customer.

At each level, the retailer simply offloads responsibility to the next level to check the identity of the customer. In the end, if the customer buys something using prepayment, for example, or pays by cash, there is no strong incentive to check their identity. Sometimes, the end-user buys online and it is difficult to check the real identity and the payment. They could use fraudulent payment, such as a stolen credit card.

The principle of checking the identity of the customer is really important. The question is enforcement. In reality, there are certain limitations on how far you can actually enforce it.

Viscount Colville of Culross: That is very interesting, and quite scary. Is it not possible, with this great pyramid of reselling of numbers and mobile phones, to mandate the telecoms company to register the mobile phone owner, and the retailers, both online and in the real world, so that there is some possibility of knowing who owns the phone, even when it gets to the very end of the chain that you have just described?

Professor Feng Hao: The question is: how does the user prove their identity? There is no central identity system. Even if you register the number with a particular user, that user may use a false identity. You cannot really trace the user. That is the fundamental problem.

In some countries, like South Africa, because of the difficulty of checking the identity of a user, the Government are thinking of introducing biometrics. Even with biometrics there are certain limitations, and you could introduce more problems. If you check the biometrics of the user, you need a central database of biometrics, which could invite other problems on privacy, so you can see that checking the real identity of a user is a fundamentally difficult problem.

Viscount Colville of Culross: With the Online Safety Bill that is going through Parliament at the moment, there are increasing pressures for verification identification, particularly for children, and there is talk of doing it for adults as well. If it is possible to do the verification online—to have forms of identification that satisfy the ISPs and Ofcom about the identification of the user—is it not possible to use something like that to work with mobile phone companies to ensure that you have an identification for the final user of a telephone number?

Professor Feng Hao: Within the UK, it is possible to have multiple checks with addresses and bills, but for users from overseas it is much harder. You can ask users to provide identifying documents, but, as I understand it, you still need to check the accuracy of those documents, and that means that doing it remotely is challenging.

Viscount Colville of Culross: You are saying that you think it is possible to do that in the UK, which would at least give people who are receiving these telephone calls some idea that a UK number—after we have, we hope, stopped spoofing—belongs to a real UK user and, therefore, you will be able to identify back who that user is.

Professor Feng Hao: Yes, it is a balance. The tougher you make the checks, the more difficult you make it for the criminal, but it is also more difficult for legitimate users. When they want to buy something, they have to provide so many proofs, because there is no central identity database that you can easily check. We have to consider that balance.

Adrian Gorham: When people take out a service, we go through credit checks. The biggest financial loss to us when it comes to fraud is identity theft: it accounts for probably 90% of my losses. We need to give service to customers when they come into a retail store or go online, but we do not want to be subjected to fraud, because that is a total loss to our business, and it has an impact on the legitimate customer whose identity has been stolen.

It has two impacts, one of which is on the consumer. They will not lose anything financially, but it is still an inconvenience to them because they have to get their credit rating resolved and so on. Anything that allows us to know our customers and ensure that we are not being defrauded is good news, but it is very difficult. The fraudsters are very good. They are very good at forging documents or, if they have committed a cyberattack, they have all that personal information.

Viscount Colville of Culross: We have heard quite a lot of evidence about identity theft, and it seems to me incredibly significant in the whole world of fraud. Would it not be useful for the telecoms companies to be mandated to do those checks and for there to be a central ID base by which you could try to defeat the identity fraud?

Adrian Gorham: If somebody came up with a central database that we could go to and verify that the customer we are dealing with is genuine, we would absolutely want to use it. But this is difficult; it has been around for a number of years and affects many sectors. It is not an easy one to crack.

Viscount Colville of Culross: What about mandating the telecoms and mobile phone companies to register the final user?

Adrian Gorham: Looking at mobile, there is a difference between pre-paid and post-paid. Pre-paid was brought in as a government initiative to help people who could not get through credit checking to get a mobile phone, so you might start to bar a lot of members of society from being able to get a device and a phone. Secondly, the fraudsters are very good. They steal other people’s data. We think we are talking to the genuine individual, but we are not; the details have been stolen. With respect, it is not quite as simple as it may seem. We explore these things all the time. We work with CIFAS and UK banking. It is an issue that affects all of us, and we all want to try to prevent it. We work as collaboratively as we can to come up with solutions.

Viscount Colville of Culross: What solutions are being talked about at the moment to try to deal with it?

Adrian Gorham: A lot more sharing of intelligence and data. In combating fraud, the more we can share intelligence and data, the better. This is an area where we have been working with the ICO to see how we can be allowed to do more of that. The sharing of intelligence is the main thing, because if a fraudster hits company A and you stop him, he will probably go and hit company C. Fraud migrates around different companies, so the more intelligence we can share, the better. Moreover, going back to the point I made earlier, we can then use that intelligence to bring these people to account, because while they are not being brought to account, they will pop up somewhere else. They always change their MO; as soon as you stop one area, they pop up somewhere else.

Viscount Colville of Culross: Okay, thank you very much.

Q236 **Lord Vaux of Harrowden:** It seems to me that there is a difference between an individual going into a shop and buying a single phone or a single SIM card and someone going in to buy 100, 200 or whatever SIM cards. Know your customer should surely be targeted at the higher-risk end. Can it not be done in those situations?

Adrian Gorham: Yes, but there are many suppliers of SIM cards. Looking at the whole retail environment in the UK, you can buy a SIM card in a supermarket, online or in a corner shop, and you can buy international SIM cards. I do not know how you would make that work in practice. Nothing is impossible, and I absolutely agree that it should be looked at, but there are many distribution channels. Sometimes we operators do not know who the customers are because they have gone to third parties—to resellers. It is a very big, broad ecosystem.

Lord Vaux of Harrowden: Okay.

The Chair: Thank you very much. Of course, at the heart of this is the point that you made at the beginning, Adrian, that the cost to the public of fraud of this nature, particularly the scam calls, is measured in billions. It does not seem unreasonable to us as a committee that the people who provide these numbers to people should take some responsibility for how they are used. I am not saying that you do not, but we are trying to think of a way of engaging that responsibility that actually begins to drive fraud down, instead of watching it increase consistently.

Adrian Gorham: If you look at trends, you will see that it is going down. There has been a lot of work by industry. In the fraud charter that we signed off with the Security Minister, there are some quite big commitments to drive it down, so we are actively working. These individuals are our customers as well; we do not want them to be defrauded, so we want to try to stop people misusing our networks.

The Chair: Yes, I understand that. We will move on.

Q237 **Baroness Kingsmill:** I am struck at the moment by Adrian saying that the solution is, "Well, let's see where the blame is. We must make the customer more alert and enforce the law more effectively". Is the source of it actually the telecoms company, as some of my colleagues have alluded to, and should the principal responsibility for the prevention of fraud in the use of their product lie with the telecoms company? I speak as a former regulator and as a director of a telecoms company. What would you say to a duty to prevent, and, indeed, an offence of failure to prevent, Mr Gorham?

Adrian Gorham: I would not encourage it, and you would absolutely expect me to say that. Our incentives are already aligned with those of our customers in terms of safeguarding retail revenues.

We are doing a huge amount of work at the moment to try to stop this use of our networks. We are purely the avenue by which a fraudster tries to communicate with the other party. These days, it is either on the internet somehow, which would go across our networks, or by sending a letter or meeting somebody face to face.

New legislation has just been passed: the Telecommunications (Security) Act. I do not know whether the committee has looked at that. It has been driven very much by government officials and the NCSC, and is about how we design, build and operate our networks so that they are more resilient and less prone to security incidents.

A lot of benefits are coming in the future. We are investing hundreds of millions of pounds in new frameworks that will come in over the next four or five years. I do not think we need to be incentivised or anything to protect our customers; we look to do it all the time. As this meeting has shown, it is not just a UK problem; it is an international and a global problem. We do not always have the levers that we need to address some of the issues, and that is why we have to work and be collaborative.

Baroness Kingsmill: Do you think it is enough of a defence to say that you are just the pipes? The gas companies, for example, stopped having the sort of gas that enabled people to commit suicide. Do you think there is more that the telecoms companies could do? If you have a regulation that says, "This is what you must do", you are more likely to take effective action. After all, you have huge amounts of resource compared to the individual customer or, indeed, the law enforcement authorities.

Adrian Gorham: We do, but I still believe there is other low-hanging fruit that we should absolutely be exploring. We are doing a lot on our networks to try to protect customers, but there is a lot more that we should do, overall in the UK, to spread awareness to customers of these types of scams, and with other partners try to drive them down.

Baroness Kingsmill: You will see the thrust of what we are thinking about in some of the questions that you have been asked. Anyway, thank you very much.

The Chair: In terms of low-hanging fruit, in October 2021 Ofcom asked phone networks to block internet calls from overseas if they pretended to be from UK numbers, and it gave some advice about that. As far as we understand, the only provider that implemented this measure was TalkTalk, which said in a report that it had seen a 65% reduction in complaints about scam calls following the implementation. If that is correct, why do the other members of your organisation not implement it?

Adrian Gorham: Different operators are working on different solutions. One of our commitments is to roll out spam protection for customers on the networks, and we are on track to deliver it. All the operators have that technology in place now and it is just a question of going through the processes of tuning and so on. It has moved on quite a lot since TalkTalk was the first out of the trap, as such. All the operators have solutions in place now. That is why, if you were to look at the current numbers, I believe you would see that they have been decreasing significantly as operators have rolled out those technologies.

The Chair: If I understand your evidence, nobody else except TalkTalk could do that, because they did not have the technology and TalkTalk had it, but now you all have it.

Adrian Gorham: Different companies trial different technologies to try to resolve these issues, and the timing of implementation is always different on the networks. I am not close enough to the detail on that, or the TalkTalk solutions.

The Chair: Maybe Professor Hao knows about the technology. Do you know about the distinction between TalkTalk and the rest of them? Was it down to technology, or was it something else?

Professor Feng Hao: Blocking a number is relatively straightforward. You can see when the call comes from the gateway, and if you know that it is an international call you can have a policy to decide what you want to do. That is straightforward.

The slightly harder part is that you need to distinguish whether the call is a legitimate modification of a number or a malicious modification of a number. That is a bit harder. In the UK context, a lot of call centres are overseas, in India and other countries, and if they call a number from their original country number no one in the UK would pick up the call because they do not want to answer overseas calls. They have legitimate reasons to have a UK phone number; there are legitimate uses for changed numbers.

The telecom companies have some solutions, but they should do a lot more. So far, what they have done is the minimum and driven entirely by revenue. If they block more calls and that affects revenues, they will not do it, or they would not have the incentive to do more because that would drive calls to other competing telcos. The key problem is incentive. There must be a government initiative to encourage telcos to do more.

The Chair: Thank you. That specific initiative came from Ofcom, and it was for blocking internet calls from overseas if they pretended to be UK numbers. It was very specific, and Ofcom gave certain advice. It seems that TalkTalk took it and did it, and had a dramatic reduction. I am trying to find out whether this is a technology issue or a willingness issue, but maybe we should explore it in correspondence. In the interests of time, we will move on. Baroness Bowles has the next question, which is about incentives.

Q238 **Baroness Bowles of Berkhamsted:** I would like to comment first on that last point. I do not see that there is any legitimate reason to pretend to be where you are not. If you are being serviced by a UK company but the service is coming from abroad, it is legitimate for you to know that. Anyway, that is just a comment.

I would like to explore compensation issues further. Some organisations such as banks and online platforms are obliged to pay more compensation. Adrian, I am sure that you will say that you could not vote for that, but, realistically, what is the difference? Are there circumstances when telecoms companies pay voluntary compensation because their platforms or services have been used for fraud? Does that happen at all?

Adrian Gorham: I will use an example. I said earlier that I had an SMS message and a scam on me, so let us run through that one. That SMS came from somewhere on the globe; someone sent me a message purporting that Simon, my postman, had failed to deliver a parcel to me today, and they needed to arrange a new delivery. That is just an SMS message that has come on our network, and the revenue we get on that is small—a penny, or whatever.

I have not taken any responsibility. I have clicked on the link, when I should be thinking, "Is this fraud?" I have gone through and entered my name. It asked me for my address and date of birth, and it all looked like the genuine Post Office website. It then asked me if I would like to redirect my mail and when I would like it redelivered. I picked a date for next Monday when I knew I would be at home. Then it said that there was a redelivery charge of £1.20, and of course it wanted my credit card details. Had I put those details in and been defrauded on my credit card for £2,000, should it be the telephone operator that is liable for that cost? I do not think so. There are so many different parties involved, and responsibility, that I think that is probably harsh.

Baroness Bowles of Berkhamsted: That goes back to the previous question on failure to prevent, in that if there are checks in place to filter out what can reasonably be filtered out, maybe you would not be liable, but if you have done nothing maybe you would.

Adrian Gorham: That is what you get with legislation. With respect, we believe that we are doing all we can to try to stop this and protect our customers. That is to our advantage. Sometimes, additional legislation can just incur more costs, slow processes down and not actually be in the best interest of customers.

Baroness Bowles of Berkhamsted: You reckon that as much as can be done is absolutely being done. You referenced in answers to previous questions that trials are going on; there is TalkTalk and others. Once the trials by the different telecom companies have got to some maturity, will they be pooled so that everybody gets the benefit?

Adrian Gorham: No. To be clear, we are going to roll out the best solutions to protect our customers, but they will not be fit for purpose long term. I have worked in security and fraud for 40 years; I used to go out and catch people committing fraud. It never stops; it evolves all the time, so we have to continually develop our ability to protect our customers. Yes, we will roll out these solutions, but there will be better solutions in the future. When we get to new technologies, we design out these types of scams. That is what the networks do as they move to the next evolution. This is an onward journey. It will not disappear.

Baroness Bowles of Berkhamsted: So why are they still trials at the moment? Is that because you were late to it?

Adrian Gorham: As I said on Lord Browne's question, I would have to check with Ofcom because I think it has now all been implemented, so it has moved on a bit. I am not sighted on that level of detail.

We are probably going a bit off track. All the operators now have these solutions in place and the numbers have come down dramatically. I just do not have that information to hand.

Baroness Bowles of Berkhamsted: In answer to an earlier question—I think from Lord Young—you said that there was not much benefit with regard to scamming, because you had to spend to try to stop it. Are you saying that you spend more trying to stop it than you would gain from the fact that you were charging for services? Have you any idea what percentage of income comes through scammers if they have thousands of SIMs and all this kind of thing going on? You are getting revenue. Do you know what percentage of your revenue comes that way?

Adrian Gorham: The answer is no. I do not think I said that, because of the small amount of money, it was not worth us spending money on it. I honestly do not think that is what I would have said.

Baroness Bowles of Berkhamsted: Sorry.

Adrian Gorham: If I said it, I apologise. It is a very, very small amount. I am trying to give an industry view, but in my own organisation well under 1% of messages could be scam SMS messages. It is a very small amount. Proportionally, it causes us a bigger problem, because I am sitting here today and it is affecting our customers. We are spending millions as operators rolling out solutions. It probably far offsets what we are earning from that very small amount of revenue.

Baroness Bowles of Berkhamsted: I think that is what you said to Lord Young—that you are spending more than you are getting.

Adrian Gorham: In my view, the amount of time and effort we are putting in, going to the joint task force and so on, shows our commitment.

Baroness Bowles of Berkhamsted: Unless Professor Hao has anything to add, we may have completed that question.

Professor Feng Hao: In a lot of telephone frauds, the telephone companies or telcos are in the best position to protect customers. They have the metadata, not just the phone numbers—where that phone number comes from, where it goes next. They have more data, so they are in the best position to protect the end customer.

Wangiri fraud, for example, which Adrian mentioned earlier—you get a missed call, you call back and it turns out to be a premium rate phone number—could be stopped or mitigated at the telecommunication level. They have the data. If it does not stop and the user has been tricked into calling back the number, who is liable? In the UK, as far as I know, Vodafone compensates users for this kind of loss. That is a really good initiative and it should be extended to other telecom companies. That would align incentives for the telecom company to be proactive and protect the end-user.

Baroness Bowles of Berkhamsted: Presumably, the moral there is that if they are proactive or compensate in that kind of way, if they are essentially doing it voluntarily, it would fend off failure to prevent requirements.

Adrian Gorham: To be clear, all the operators do that on Wangiri fraud. We are not here to profit from fraud in any way at all, so we do not charge the customer. If a customer has a call come up on a bill and it was because of a Wangiri, we will delete that call from their bill and we would not charge them for that. I believe that is all the operators; it certainly applies to my company and always has done. So the customer would not suffer a loss.

Baroness Bowles of Berkhamsted: How would they know if they do not inspect their bills regularly?

Adrian Gorham: If they do not inspect them, it could slip through the net. When we spot that there has been a Wangiri fraud, we can look on our network and see where calls have been made to ensure that we do the credit so that the customer is not at any financial loss. Wangiri fraud is a very, very small issue these days. It used to be a bigger issue years ago. These days it is quite rare, but we are quite resilient in how we deal with it and protect our customers.

Baroness Bowles of Berkhamsted: When you find a fraud like that, do you automatically compensate without there being need for a claim? You scan your networks and your customers.

Adrian Gorham: It is because there is a call charge for a call they have made using our services. You have to remember that with the other frauds we are talking about fraud that is on somebody’s credit card or fraud to buy a car. It is well outside my ecosystem.

Baroness Bowles of Berkhamsted: Understood, but if it is in your ecosystem and you can track it, you would make sure that customers are not charged extra.

Adrian Gorham: Wangiri fraud and fraudulent applications are by far the biggest loss in the industry. We recompense our customers. For that, it is not a problem.

Baroness Bowles of Berkhamsted: Okay.

Q239 **Lord Sandhurst:** I want to ask about collaboration, Adrian. The CCSG, your group, has nine key actions. I am not going to ask you about all of them. This is on actions 5 and 6. Action 5 is sector information sharing. Action 6 is systematic sector analysis of shared fraud and other intelligence.

My questions fall into three parts. First, how far have your group and companies got with those two in particular?—[*Inaudible*.]—Secondly, what activity is being undertaken to improve information and data sharing? Thirdly, what is happening vis-à-vis the ICO to try to get exemptions on data sharing, and—[*Inaudible*.]—what is being done about setting up, for example, a cryptographic system with blockchain—something Professor Hao mentioned—to keep it secure and private? I hope you can see where I am going.

Adrian Gorham: Yes. I am not sure about other people on the committee, Lord Sandhurst, but for me you were breaking up a little during your question.

The Chair: I think we all experienced that. Did you get the gist of his question, Adrian?

Adrian Gorham: Yes, I did. On collaboration, there is engagement with the ICO's office on our sector information-sharing approach, because we want to make that better and share more. The ICO has been supportive in those conversations, and we anticipate completing a new model on how we are going to approach it and get it all signed off by the ICO later this month. We will then move in July to an implementation of the improvements to that sharing of data.

I would have to refer your question about blockchain to the people working on that particular action on the fraud charter and the working group to see if it is something that could be considered would add value.

There is a lot more going on now with the ICO. We need to work within the law, and sometimes that can be a barrier or a reason why people do not want to share information and data. I have always been a believer that if it is being used to fight fraud, we should absolutely proactively do it.

Lord Sandhurst: Are there any barriers to this that you would like removed? In other words, would you like us to recommend that the ICO gives you certain exemptions which at the moment it does not?

Adrian Gorham: Yes. Everything we do is within a legal framework. As companies, we have to work within those frameworks. The desire of people working in the sector is to protect customers. We would always like to move faster, and sometimes controls that are there for legitimate reasons when legislation is passed can slow things down. Yes, I would like to be able proactively to share data to prevent fraud.

Lord Sandhurst: Instead of listing them now, could you write to us afterwards with a list of exemptions you would like the ICO to grant you, which you do not have at the moment?

Adrian Gorham: I will do that. We will provide written evidence of where we think they are. I think they are aware at the ICO. In fairness, we have very good open dialogue with them.

Lord Sandhurst: It would be very helpful to know where a prod from us might help.

Adrian Gorham: Okay, thank you.

Q240 **Lord Gilbert of Panteg:** Professor Hao, you are in the hot seat for this one. Thank you very much for your expertise so far. I want to pick your brain on the role of fraudulent internet domain names in this space. We have heard quite a lot of evidence about phishing scams that divert people to false websites.

We heard of one solution, particularly in banking, where with rapid information sharing between players in the system, fraudulent bank domain names have been stopped at DNS level by network operators. I am interested in what more we can do in that area. You have written on and researched the issue of fraudulent domain names and identified that it is probably more a problem on mobile devices than on laptops or PCs. I can see that on a mobile device it is not quite as clear what is in front of you, so clicking around to check out the veracity of a domain name is more difficult.

How significant a problem is it? How do fraudulent domain names contribute across the piece to a variety of different forms of fraud, and what could be done? Could knowing your business customer be an important part of dealing with this? From a number of the questions asked today, it seems to me that knowing your business customer is potentially quite important and may be here.

Professor Feng Hao: Thanks for the question. I wish there were a silver bullet for this problem. The problem has been known for many years. The phishers register domains using all kinds of techniques. It is commonly called typosquatting; for example, they choose a specific bank and change one or two characters. It is difficult for domain registers to detect. Sometimes they can block it, but because it is very difficult to make it comprehensive it sometimes just goes through.

Criminals never use their real identity; they always use a stolen identity to register the domain. They do not register it in the UK; they register it overseas. They use a stolen credit card to make payments, or bitcoin or an anonymous payment method. Fundamentally, it is quite difficult to check their identity, because they do not want you to check and they have all these techniques. The best the internet domain, the hosting company, can do is to monitor the traffic and, based on the user report or the traffic, see whether it is likely to be a fraudulent website, but in many ways criminals can work around it. I wish there were a silver bullet, but it is a fundamentally difficult problem.

Lord Gilbert of Panteg: Is there anywhere, as a consumer, that I can quickly look up a domain name and see whether it has risk factors attached to it? Where it is registered might be a risk factor. The fact that the owners of it are not verified might be a risk factor. Is there a simple website or app I can use to do that?

Professor Feng Hao: Yes, there is public information on the website. You type in the domain and you can see who has registered the domain. Usually people who take such proactive steps to check the domain name are not victims of fraud. It is only the people who do not bother to do that kind of check, because they do not have the expertise, time or incentive; they are the targets and the victims.

Often, phishing websites are short-lived. They do not last long, because it takes time for the activities to be detected. After a day or two, they get the fraudulent transactions and make enough money, and if it is detected and blocked, they just open another domain.

Lord Gilbert of Panteg: That is registered.

Professor Feng Hao: Yes.

Lord Gilbert of Panteg: If it had just been registered today, that would be a risk factor in itself, would it not? That would be a flag. Maybe people do not use these tools because they do not know they exist and they are not very simple. It seems to me that a straightforward app on your phone that had all this data and a flag against it as to where there is a risk factor might include, for example, when it was registered. If it were registered today, that might carry an automatic red flag.

Professor Feng Hao: That is a good solution. There are already solutions similar to that, for example, on mobile phones. You can download apps that can check these kinds of website and it gives you a flag warning that the website is likely to be fraudulent. With a browser, you can download some plug-ins to do that kind of check. But users have to take proactive steps. They have to install software on their PC, and not many people are comfortable with doing that.

Lord Gilbert of Panteg: It is a bit of a common theme: the tools are there, but people do not really know enough about them.

Professor Feng Hao: Yes. It relates to an earlier point made by Lord Allan: that there are a lot of good solutions at the users’ end, but they are not integrated into the system; the user has to do something at their end. It would be far more effective if these protective mechanisms could be integrated into the network level as part of the telco system.

Lord Gilbert of Panteg: And it should be very visible. If you are in a high-risk place on the internet, it should be in the corner of your screen at the time when you were likely to be at risk.

Professor Feng Hao: Yes.

Lord Gilbert of Panteg: Thank you.

Adrian Gorham: Certainly, as operators, the device manufacturers have a part to play in this with the security of their devices—how inherently secure they are—and that varies. We wrote to one recently to ask them to consider increasing the security. Consumers do not want to see the security wrap; they want it seamless. They just want to trust that when they click it is all right. Telling consumers to download different bits of software and check things will be very hard to communicate and get them to do. Building it in has to be the way forward.

On the ISPs, we have talked about 7726 getting far more usage. When people report the URLs, if they are on our own intellectual property, if they are within our own domain as a company, we bar them immediately. If not, they go to the NCSC, which goes out to the ISPs to get them barred. Again, it is not as effective when it is international, and actually—

The Chair: I am sorry to interrupt, but we have another witness for another session and we have to respect that. I appreciate that there are lots of things still to say and there are a couple of important questions that we would like to ask. If we may, we will write to both of you with those questions. In any event, you have indicated, certainly Adrian has, that you would write to us about one or two things. We will remind you of what they are.

Adrian Gorham: Yes.

The Chair: I am sorry to do this, but it is a credit to both of you that you have engaged with us so well. I want to wind this up by thanking both of you very much indeed for your time this morning. Believe it or not, some people claim to enjoy giving evidence to Select Committees. Others are a bit more honest and admit it is something they would rather not be asked to do. Both of you have taken time to prepare and we appreciate that. Whichever category you fit into, we are very grateful to you for coming and being generous with your time today. There will be follow-ups for both of you, so thank you very much for that.