HOUSE OF LORDS

Select Committee on the Fraud Act 2006 and Digital Fraud

Uncorrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 10 March 2022

10.45 am

Watch the meeting

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

Evidence Session No. 5 Virtual Proceeding Questions 44 - 51

Witnesses

I: Alex Towers, Director of Policy and Public Affairs, BT Group; Hamish MacLeod, Chief Executive, Mobile UK.

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.
2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.
3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witnesses

Alex Towers and Hamish MacLeod.

The Chair: Welcome to this second evidence session this morning of the Fraud Act 2006 and Digital Fraud Committee. A transcript of this meeting will be taken and published on the committee's website. You will have the opportunity to make corrections to that transcript where necessary. Thank you for joining us. We have Alex Towers, the director of policy and public affairs at BT, and Hamish MacLeod, the chief executive of the trade association Mobile UK. Without further ado, I will hand over to Baroness Taylor for the first question.

Q44 **Baroness Taylor of Bolton:** Good morning to both of you. We have heard a lot about fraud, and it is very clear that one of the major problems is the question of authorised fraud. The banks have been very keen to explain the problem from their point of view and tell us what they are doing, but clearly telecoms companies—with texting, spoof messages and all the rest of it—are a very big part of this, so you are right at the centre of this problem. Can you give us some idea about what you think telecoms companies can do to protect consumers and to disrupt what is actually a very big fraud business?

Alex Towers: There is quite a lot we can do, and although we have done a lot, we can still do more. As you say, it is a big problem. We would estimate that the scale of the problem is in the millions of cases every day, if you add up the total of bad calls, whether it is spam or scams that come across either the voice network on landlines or in text messages. The pandemic in particular was a bit of a wake-up call in recognising both the scale of the problem and that perhaps we had not quite done enough yet to address some of this.

Overall, the numbers and scale of fraud are up 20% or so across the economy, which is not just an issue for us; in that grim period, some of our most vulnerable customers were at home on their own and vulnerable to this really miserable form of criminal targeting. That has spurred us and across the industry to do more, and Hamish can say more about how we have tried to join this up. Going back many years, we already had all sorts of things that we have offered free to our customers—call protect, caller ID, web protect and virus protections—but the scale of the problem remains.

We have been focused on working quite closely with the financial services industry, the Government and law enforcement. This is a team effort. Since last summer, we have implemented what we call Spam Shield across the EE network, which is trying to block out at source a whole load of the problems of spam and scam text messages, with quite a lot of success. We have blocked over 80% of those spam texts, and the numbers of reported scam and spam text messages fell by over 90% in that period, so it is clearly a very good thing to have done. It has not eradicated the problem altogether, but it is a big step forward.

The next thing that we are fixed on doing, and the industry and indeed Ofcom are also fixed on doing, is trying to tackle the voice call problems that are often tied up with international calling networks. We can perhaps come on to talk about that in a little bit.

On the authorisations and how we work with banks on text messages and identification, which is probably the focus of your question, we do a lot with the banks. We do a lot in trying to make sure that, when we acquire new customers, putting them on to our network and giving them contracts, at that point there are legitimate credit checks. We talk to the financial institutions about how to improve those sorts of processes.

We also talk to them about how to improve their own processes in things such as two-factor identification, where there are potential weaknesses. If text messages are passed through those sorts of processes for authorising payments, there is some stuff that we can do. Obviously, there are alternatives to using SMS as a form of identification. Some banks use app-based systems, which is one approach. Where text messages are being used, we now do quite a lot more, in particular to identify for the banks where a number is associated with a recent swap of a SIM, for example, because that is an obvious indicator that there could be a problem and there might be something suspicious going on. We help with that.

More broadly, we do a whole load of work, including through an organisation called Stop Scams UK, which we set up with lots of the banks and other telcos to try to share broader trends on the pattern of criminal activity and to identify the digital fingerprints that we can share with them to try to root out some of those problems. There is also clearly a dimension to this about sharing that information with law enforcement. There is loads to be done and it is constant ongoing activity.

I will stop talking and let Hamish answer in a second, but one other obvious general point to make about all this is that we will never remove the criminal intent and criminal actors from the scene here. There is a slightly unpleasant whack-a-mole-type element to all this activity. We are doing what we can to push down at source on rogue calls and rogue text messages. We now see people transferring their criminal activity into social media platforms as an alternative. The more we clamp down in one area, it pops up somewhere else, unfortunately.

Just as in the pandemic it was pretty grim to see people being exploited when they were vulnerable at home or targeted through their interest in vaccines, or whatever, now you see fraud in fake charitable fundraising for Ukrainian charities, for example. There will always be something to try to tackle, but wherever we can try to remove the obvious and easy pathways for people, that is what we are trying to do.

Hamish MacLeod: I will focus my comments on the telecoms fraud sector charter, which no doubt you have been told about. This is a Home Office initiative that was kicked off—

Baroness Taylor of Bolton: I wanted to come back on what Alex was saying. Could we focus a little on what he was saying, because it seems to me that the whack-a-mole approach is almost admitting that the fraudsters will always be one step ahead and there will always be a limit to what you can do? Why can you not do more about the bulk calls from abroad? Why can you not do more about the problem of fraudsters keeping the line open while people allegedly phone their bank and things of that kind? This has such a devastating effect; it is not just the financial loss but the personal loss. People feel stupid when they have been duped, yet there seems to be a sort of resignation that it is going to happen one way or another, and we are always behind the curve.

Alex Towers: It is not resignation at all, and you are quite right to focus on those things. We are in the process of implementing a whole new set of technology on voice calls. From this summer, from June, across our BT landline network we will block out a whole load of spoof calls that look like they have a UK number but originate from elsewhere in great numbers, which will be a big step forward. We are in the process of upgrading the old analogue landline network to a digital equivalent, which is not without its separate complications, but we are going through that process. As we go through that, we will improve the way the process works with more efficient and effective AI-based provision of that service, which will track and provide alerts directly to customers in real time on what is going on on their system. There is much more we can do there.

Ofcom is also actively thinking about this and published a consultation last month that proposes to make the sort of approach that we and BT will implement mandatory across the rest of the industry. That clearly is also a good thing to do, because the whole industry is only as effective as the weakest point in the system. It absolutely is something we can do.

The other thing we would point out that needs to be thought about hard, and the Government are thinking about, is to try to provide a much clearer set of blocks on text messages and rogue voice calls. The next focus ought to be social media and fraudulent advertising in scams that appear on Facebook or wherever. We have been saying for a while, as have the banks, that that is a gap in the proposed online safety legislation. Only yesterday, or certainly very recently, the Government said that they are proposing to include something on that in the legislation when it arrives.

The Chair: We will get on to some detail about the spoofing of international calls in a moment.

Q45 **Baroness Henig:** I will do that. I want to ask Hamish about the fraud sector charter and the commitments, and how you are working with those. What is coming over is a sense that there are two elements to this. There is the macro level with the commitments that you are talking about—the charter—and the micro level, where there is so much of a problem with ordinary people facing ordinary problems. How will the commitments in the fraud charter shape the landscape to help the person who is struggling at ground-floor level?

Hamish MacLeod: I think they shape the landscape a lot. Let me make a couple of points about the macro stuff and perhaps drill down into the more micro level.

On the macro, it is great that there is some transparency in relation to the fraud charter. The commitments are public and there is a way of reporting back to the Home Office on progress, et cetera. It is very good in raising the profile of the whole issue, encouraging much more cross-sectoral collaboration and collaboration between the private sector and the public sector. At the macro level, that has been very positive.

If I drill down, say, on action 2, which is particularly where Mobile UK is involved, we are essentially responsible for co-ordinating the cross-industry work to disrupt fraudulent text messaging. We are working within what we call a five lines of defence framework.

The first is about safety by design. That is encouraging our merchants to make sure that they use reliable routes for buying text messaging.

The second is at the handset. For example, for probably 18 months or a couple of years now, pretty much all Android handsets have something like a filter. It pops up and says, "This looks like quite a suspicious text message. Do you want to report it?" That has been great and has increased the levels of reports coming into 7726 very much. I will explain a bit more about 7726 in a second.

The third is in the network. Alex talked about the spam filters. All the operators are at some phase of implementing their spam text filters. We have three operational now and one in the phase of becoming operational. That has had quite a significant impact on the volumes getting through to customers.

Our fourth line is about customers and ensuring that they report to 7726. Just to remind you, in old money 7726 on your alphanumeric handset spells out "spam". We get all those reports. It is a massively important source of intel for the operators, who use this to calibrate their spam filters and to work out which is a good text message and which is bad, and for the public sector. The Information Commissioner, for example, has access to this data and can pursue people who are conducting spam text messaging.

The final line of defence is partnering with the public sector. We have the National Cyber Security Centre. If text messages come through and they have URLs embedded in them, they are sent to the NCSC for assessment. If they are fraudulent, the take-down procedures are kicked off. We also work with the police to bring people to justice who have been involved in scam text messages. There were two very significant successful prosecutions in 2021 and a further eight arrests. I do not have visibility where those arrests have got to, quite understandably, but absolutely we are very keen to work with law enforcement. That is a bit of a drilldown on what we are doing to attack text messaging.

Q46 **Baroness Kingsmill:** I will cut to the chase in the interests of saving time in getting to the heart of the matter. How do you work with other sectors and regulators to prevent fraudsters cashing out on the money? Would it be a good idea to give Ofcom the ability to charge telecoms companies for losses incurred as a result of scams passed via their networks? The banks are required to undertake reimbursement. Given the large volume of scams that happen via telecoms networks, and I speak also as a former director of a telecoms company who has experienced this, do you not think that the telecoms companies should themselves be required to contribute into the reimbursements?

Hamish MacLeod: It has to be remembered that the vectors of attack and how these scams happen is through the harvesting of personal data. The route through which this personal data is harvested is not always completely obvious, whether it is from scam advertising, scam text messaging or whatever, so that connection is not necessarily there.

Having said that, we will invest hugely in anti-fraud measures, in the spam filters that we have just talked about, in working with the police to put together intel packages and what have you. I do not think I am in a position to volunteer on behalf of the industry for what would amount to extra funding, but certainly we will invest in helping the police to disrupt this activity as much as we can.

The Chair: I will take that as a no, you would rather not reimburse, which I can understand on behalf of your members. Let us drill down into some more of these disruptions.

Q47 **Baroness Bowles of Berkhamsted:** I will elaborate where I am going so that you can answer it all at once. First, what is the scale of international telecoms fraud? Can you give us some figures on that? If you do not have them to hand, you can send them to us. How many calls or messages come from overseas, and, in percentage terms, how much of it is that?

We have heard in the previous session that the UK is a particular target for APP. In drilling down further into how you are going to address that issue, we come up against the protocol of SS7. This means that we cannot utilise the advances that they have been making in the US until it has been upgraded, and it seems to be unclear how and when anything can be done. Ofcom says that it will not be possible until 2025, but there will still be 2G and 3G bits of networks hanging around for much longer than that, and some probably will not be gone for 10 years.

Alex, you said earlier that you have removed the obvious and the easy. Obviously, some of this is about investment, and it is investment in the infrastructure rather than specifically addressing fraud. Is part of the problem the fact that that has not been done?

Alex Towers: Shall I start with the numbers? It is not easy to have very precise numbers, it has to be said. These are ballpark figures, but they are also very large, which is the key point. Crudely speaking, the majority of the problem with voice calls currently is that it is international in nature, while the majority of the issues with text messages tend to be a bit more UK focused. That is very broad brush, but I think it is accurate.

As regards numbers, across our fixed-line voice networks we see millions of calls every day that are in one way or another bad calls. By that, I group together nasty, scam-type stuff with the more spam robocall nuisance, annoying kind of stuff. It is difficult for us to distinguish one from the other at source, as it were, but it is obviously very large numbers. The Ofcom research showed that roughly three-quarters of the population in the past few months said that they had been aware, either on their landline or their mobile phone, of some sort of spam or scam or nuisance sort of stuff.

The numbers who complain are quite a lot smaller. One issue here is to try to do more to promote ways in which people can report some of this stuff, because through reporting we get intelligence and we can try to do more to act and to help with enforcement. People can report things to the 7726 number, as well as to Action Fraud at the police end of things.

Every week, BT and EE get roughly 20,000, when you add together calls to our contact centres and things reported to the 7726 line. That is a lot lower than what we know the scale of the problem is. That is largely because for lots of people, and I certainly include myself, it is very easy to ignore it and move on, knowing that it is something you should not pay any attention to. That probably explains the difference in the numbers.

Baroness Bowles of Berkhamsted: Is there a possibility of having a spam button that people could automatically press so that you could harvest that?

Alex Towers: That is the sort of thing we should think about. I do not think we have cracked this bit. Yesterday I talked to people from Ofcom who are also interested in what more we can do to try to promote it. They know that the wider public really care in a generalised way about how the telecoms system works. There is generalised anxiety about it, but perhaps not quite enough understanding of where to go to report it, how to highlight the problem, or whatever. I think that between the industry and the regulator we can do a bit more about it.

Baroness Bowles of Berkhamsted: Hamish, on the international side.

Hamish MacLeod: On the text messaging side of things, the way you buy text messaging is an international market. It is not always obvious, even if the text messaging comes from overseas, whether that is an overseas-initiated issue for UK domestic customers.

I do not know if it would help to go into the more technical aspect, but there are two essential ways of routeing text messages. There is P2P—person to person—which is just you and me texting each other about when we are going to have lunch and that sort of thing. The abuse there is that people buy what they call SIM farms, which are devices through which you can send tens of thousands of text messages in very short order. They are not lawful, but they are extremely hard to detect. However, the spam filters do have facilities that can set rules that will try to minimise the damage that a SIM farm can cause.

There is also the A2P route, which is application to person. If your doctor or dentist are sending out reminders about appointments, or the Government are sending out Covid booster reminders, they would be more likely to use an A2P route. It is really important that we encourage our merchants to understand how they are doing that and that they go to reliable providers, not just the cheapest. In an ideal world, they will tell us which routes they are using, because in that way we can watch the routes they are using, let their legitimate traffic through and just block stuff coming from other directions. That is why working with our merchant partners is a very important aspect of tackling this.

Baroness Bowles of Berkhamsted: But neither of you has said anything about SS7 and investment, and how to make the systems better, rather than how to tackle what is a problem because of the system we have.

Alex Towers: That is a totally reasonable question. We are constantly trying to invest in new systems here. That is absolutely part of the answer. That is what we have done with our Spam Shield. That is what we are doing with the blocking of voice calls that will be introduced later in the year. As I say, part of the big investment that we are making in upgrading the way the landline systems work from analogue to digital is to try to make that whole system more resilient, and to allow it to have a better level of protection for consumers, because it will create a smarter form of call blocking and screening and a more intelligent way to do that. We think that is important.

Indeed, as you mentioned, over time—these are not instant processes—we are going through the process of upgrading and will eventually retire what we call the legacy networks of 2G and 3G. We are upgrading from superfast broadband to full-fibre broadband. We are the largest capital expenditure investor in the country. We are putting a huge amount of effort into trying to make sure that we have the most up-to-date systems and networks possible. It does not remove every vulnerability to rogue actors, obviously, not least because some of this, unfortunately, is about people exploiting human weaknesses and human behaviour, and it is a combination of technology and manipulation of individuals that goes on.

I would add to what Hamish said on SIMs, SIM farms and all those sorts of things. Some things can be done to try to help with that. We have now introduced some limits on the number of text messages any one SIM can send in a day, which is still a high limit—it is 2,000 or something—but it counters some of the really crazy stuff that Hamish referred to. We have stopped selling bundles of £5-worth of mobile data at a time. We try to clamp down on third parties who are selling data upgrades and packages on our behalf, so that when we see people doing suspicious or nefarious things we stop working with them. There are also ways of trying to squeeze and tighten all those things. Again, it does not totally eliminate the problem, but it does quite a lot to reduce the potential.

Q48 **Lord Gilbert of Panteg:** I think you can answer my question quite briefly. You have talked quite a bit about how business is getting its act together and co-operating and co-ordinating efforts. I want to explore a little how you work with government. I do not know whether either of your bodies is a member of the Economic Crime Strategic Board. It is the lead public sector-private sector forum. I wonder how it works. It is supposed to be led by the Home Secretary and the Chancellor. Perhaps you can comment on your understanding of how effective it is.

Also, briefly, would you tell us, from your observation, how joined up government thinking is across the fraud piece, including the aspects that most concern you?

Hamish MacLeod: We are not formally members of the ECSG, but we have been broadly consulted on the production of the 10-year fraud strategy that the Government are working on. We are also pretty engaged in how we communicate to the public about this. This is very challenging, because fraud has many facets—dating fraud, investment fraud, all sorts of things. You have to work out a way of making the customer fraud-aware without scaring the living daylights out of them so that they never go on the internet. It is a fine balance.

At the moment, they are doing some research into how best to approach that and how we can have a holistic approach to resilience—making customers or making the public more resilient to the whole thing, as I say, without putting them into a state of paranoia, which would be a very poor outcome. On the industry side, we provide information specific to us, but this needs to be at a much more macro level.

It is a complex field. I think it is getting better. We have the Joint Fraud Taskforce, the ECSG and the FCSG, looking specifically at the communications. It is multifaceted. To some extent, you need to slightly break these things down and tackle them in a manageable way, but you also have to work at the macro level and have an overview. I do not envy their task, I must say.

Lord Gilbert of Panteg: Briefly on that, where in government do you sense that the political leadership is coming from? Can you clearly observe who is getting a grip of this at government level?

Hamish MacLeod: Our prime contact on this is the Home Office.

Lord Gilbert of Panteg: Do you think it is pulling it together effectively across Whitehall?

Hamish MacLeod: I think the sector fraud charter that telecoms and various other sectors have was a very positive move forward to improve transparency and collaboration between the various parties, yes.

Lord Gilbert of Panteg: Alex, how is working with government working out for you?

Alex Towers: I agree with Hamish. I would say that probably, as the industry, there is renewed focus and energy behind this since the pandemic, led by the Home Office, but with the DCMS and law enforcement very closely involved. I think we have enough forums for joint working and task forces and charters. There is a lot of stuff there.

Lord Gilbert of Panteg: That is my point: there is a lot of stuff. Is somebody gripping it and pulling it all together so that it is one meaningful set of work, or are they just a pile of programmes all of which you have to input into?

Alex Towers: I think they are consistent with one another, which is all we would really ask for.

Lord Gilbert of Panteg: No, we can ask for more than that. We can ask whether they are joined up and all heading in the same direction. Not being inconsistent is the minimum I think we would ask for.

Alex Towers: Okay, I think they are heading in the same direction, actually. I am sure there is more we can all do, but there is no issue with that. The one you started asking about, the strategic board, is clearly very high level, but we have relationships at every level of the chain, which is what makes this stuff work effectively, I think. We are part of the fraud charter, as Hamish has referred to. That has involvement from the DCMS, from Ofcom, as well as from the Home Office and law enforcement. We are part of the NCA's National Economic Crime Centre, which is looking at the specifics of cell, voice calling and SMS scams, which has been very helpful. We have links into the police at working level. The City of London Police in particular are very helpful in helping to escalate specific things when we have specific intelligence to pass on. As Hamish also mentioned earlier on, there is the NCSC.

All these things are trying to push the same points and head in the same direction, and all of them, I think, have had renewed energy and effort put behind them, and indeed senior political emphasis in the past 18 months to two years, and we now just have to crack on with it.

Lord Gilbert of Panteg: That is interesting, thank you.

Q49 **Lord Vaux of Harrowden:** You have talked about the various ways of controlling the calls and all the rest, but, frankly, we are all bombarded with huge numbers of calls and texts, and I, at least, have not seen any reduction in that recently. All these calls and texts are presumably paid for by somebody. Who receives the income, and how much money is the industry actually making out of all these fraudulent calls and texts?

Secondly, would mandating the registration of phone numbers be a solution to deter fraudsters? If not, what might be? I look at the banks. They have "know your customer" rules. Should the telecoms industry have something similar?

Hamish MacLeod: To be honest, part of the problem is that text messaging is now incredibly cheap so the answer is that it is no longer a big revenue stream for operators, and that is for what is genuine. We have to remember that about 50 billion text messages are still sent a year. That is way, way off its peak. It is so attractive to fraudsters partly because it is a very effective way of communicating. That is why the Government used it a lot to remind people to get their Covid boosters, and all that sort of thing. It is pretty cheap now, I have to say. For a fiver, you can send tens of thousands of text messages.

The GSMA, our global trade body, has looked at the ID issue. Some countries insist on ID before you buy SIM cards; some do not. There is no evidence that that makes a difference in reducing this type of crime, but we worry a lot that it might create barriers to the socially excluded in accessing telephony.

I have been in the industry a long time. Only about 10% people had mobile phones when I joined the industry, and only about 80% of people had landlines in those days. The mobile phone has been incredibly effective at making sure that there is universal access to telephony and, indeed, to the internet. We do not want to put barriers in the way of the excluded, which would have no impact on the levels of crime.

Lord Vaux of Harrowden: I am actually rather shocked. We had a question earlier about how many calls are fraudulent, to which there was no answer. Twenty thousand is obviously just a tiny tip of the iceberg. You are telling me that you do not know how much revenue you make out of fraudulent activity. Surely to goodness you have some idea of the number and the money that is paid.

Hamish MacLeod: Versus the cost of all the investment that goes into—

Lord Vaux of Harrowden: Just the absolute minimum, not versus the cost. I am asking how many.

Hamish MacLeod: As to how many, the most recent Ofcom research I have seen is that about three-quarters of people report having received a scam text message. That was in October 2021, which may reflect the fact that this time last year we had a massive issue with something called FluBot, which produced a huge spike. That may reflect those numbers. Since the FluBot attack this time last year, the total reports coming into 7726 are down over 80%, so there is a demonstrable impact, and I have seen the numbers.

Alex Towers: From our point of view, as regards our total revenues, the income from any of this is not material, but clearly we definitely, desperately do not want to be making money from criminal activity if we can possibly avoid it. That is why we are putting all the investment into trying to cut off this problem at source and enormously reduce the numbers. The Spam Shield, which has reduced the reported number of scams by 90%-plus, is a really good indicator. That is why we want to do the same with our voice calls.

As Hamish was saying, we are not necessarily convinced that the answer is to insist that everyone is identified when they get themselves a phone. There are really good reasons why some people are very financially vulnerable and can only afford to pay in a certain sort of pay-as-you-go type of way. Other people might want, for good reasons, to have their privacy and anonymity protected, such as the woman fleeing an abusive relationship sort of scenario. I do not think the answer is to mandate that suddenly everyone is on a contract and identified in a more intrusive kind of way, but there absolutely is more we can do. As I said earlier, we have been trying to squeeze down the ways in which people can bulk-buy SIMs and manipulate them in all sorts of bad ways.

This goes back to one of the points that Baroness Kingsmill made earlier about where the regulatory lever is in all this. As Hamish said earlier, it is hard for us as telecoms companies to get our hands around every dimension of this problem and fix everything and therefore be liable for fixing everything. There is probably more that can be done. This is what Ofcom is thinking about, I understand: to raise the level of what is expected from the regulator as a mandated set of requirements on operators to do all the right things, to do absolutely everything we can to put the blocking and protections in place. If we do not do those things, it is totally reasonable to look at the repercussions of that, what sorts of regulatory consequences there are, where the fines are, and all those sorts of things. That is absolutely what we would expect.

Lord Vaux of Harrowden: We could push this further, but we do not have time. Thank you.

Lord Allan of Hallam: I have a quick point. For a consumer who is aware, one of the obvious things they will do is go to a popular search engine and type in who called them from a particular number. What they get back is a bunch of services that themselves often look quite sketchy. Why is the industry not offering people a really good, authoritative reverse phone look-up number so that they can see if it is a scammer who is calling them?

Hamish MacLeod: The honest answer is that that is the first time that point has been raised with me. Ofcom is currently consulting on this whole business of spoofing. It has suggested some quick wins to make sure that there is valid format of CLIs and the blocking of ones that are not in a valid format, but that does not address the spoofing issue. In other words, can you verify that the number that is being presented to you is in fact the number that is calling you? That is all about agreeing international standards, and what have you, of passing CLIs down.

Lord Allan of Hallam: It is a slightly different point. When a number is known to be from a scammer—you said yourself that people are reporting these numbers, and you have a big database somewhere—as a member of the public I want to check whether this number is in your database. That seems more difficult than it should be at the moment. Alex, I do not know if you have anything to add on that.

Alex Towers: That is a really good question. We should think about it. Ofcom should think about it. Let us take it away.

The Chair: We will obviously ask the regulators, but Hamish, or Alex, if you would like to think about that further and write to us to answer that question in full, we would be very grateful to hear from you.

Hamish MacLeod: I suspect it revolves around putting reliable information there because of the spoofing issue.

The Chair: That can clearly be probed further, so thank you for that. Lord Browne has a short question on prosecutions.

Q50 **Lord Browne of Ladyton:** It is a relatively short question. The ultimate deterrent for most crime is that you run the risk of being caught, prosecuted and sentenced in some way. This question asks what you can help us to recommend to make sure that more people are caught.

I ask you this question first, Hamish, because in your first answer you told us that in co-operation with the police you had managed to contribute to two prosecutions last year that you knew of, and eight arrests, although you did not know how many of them had been prosecuted. I have to say that, considering the scale of the problem, that seems inadequate. Prosecutions alone have gone down from 20,000 a year in 2010 for fraud to about 5,000. They have a pretty good rate of success, but it is minuscule compared to the scale of the problem. Why, in your view, are so few fraudsters who use the telecoms network to conduct fraud being prosecuted in the first place? How could we get that rate of prosecution increased? What contribution could the industry make to it?

Hamish MacLeod: We certainly agree with the head of the NECC, who said that in today’s world a greater proportion of police resources should be devoted to the whole area of fraud.

The other issue, as I understand it, and Baroness Morgan as a former Home Secretary might know more, is that the police are set up to deal geographically with the location of victims, and all that sort of thing. That is not necessarily a good way of tackling fraud and crime in the telecoms environment, where the number of victims tends to be quite small in any given area, but if you aggregate them, it is quite a few. We would certainly agree with more specialised units.

As to why more are not prosecuted, I do not have visibility of the triaging process that the police use. Would they prioritise going after a dating fraud issue over a telecoms fraud? I am afraid I just do not have that information. What I will say is that we are very happy to put intelligence packages together with the police and to help them bring successful prosecutions with whatever data we have at hand.

Lord Browne of Ladyton: Alex, perhaps you could tell us what percentage of your resources are devoted to the investigation and prevention of fraud.

Alex Towers: I could not answer that off the top of my head, but I can absolutely send you a note on it.

Lord Browne of Ladyton: It is supposed to be 1% of police resources. Do you think it is more than 1% of your resources?

Alex Towers: As I say, I do not know. I do not want to guess. That would be a silly thing to do. Let me send you a note. Certainly we have increased that in the past couple of years as part of the whole set of activity we have been talking about this morning. We also now have dedicated resources. We have a person at this end in the UK who, in liaison with the police, is dedicated to the intelligence packages that Hamish describes. We have something like 35 under way at the minute that are on the way to the police. We also now have some specialists in India, where there was a particular issue with internationally operated, criminal voice-calling networks, to provide a bit of liaison at that end. We are increasing things. Clearly, we do not have comparable resources to the police and law enforcement on this, but let me provide you with some more information separately.

Beyond that, I am reluctant, as Hamish is, to sit here and say that the answer is more police resources. That is the easy answer to every question, is it not? There is probably something about more specialist resource—perhaps a different balance of activity. It has made a difference to us, even in a small scale way, that there is now some specialist resource and a unit set up in the City of London Police to look at some of these things, and a route in for us to have that kind of liaison and those technical conversations.

There is clearly a question about whether more could be done internationally, given the scope of the criminal gangs that are the source of the problem here as well. But, like Hamish, it is very hard for me to reach further beyond that into the criminal justice system in examining whether it is operating well enough here or not.

Hamish MacLeod: It is also worth adding that this is a multi-headed hydra that we are dealing with here. Most of you will be aware that the Telecommunications (Security) Act 2021 has just gone through, so there is an awful lot of work and investment going on on that side to make sure that the networks are completely secure from hacking and cyberattack and all that sort of thing. That is a very big part of it.

Culturally, it is not just the specialists who are involved in this. It is all the front-line staff, particularly people in call centres, who are there to protect personal data. One of the vulnerabilities is being rung up and blagged out of personal information, which is sometimes incredibly inconvenient for customers who have forgotten their passwords. Although they are not specialists, that would be included within the remit of trying to protect customers from fraud.

Q51 **The Chair:** Obviously, we have issues to follow up on, and that has been very helpful. I am going to ask each of you whether you have one policy recommendation to the Government. The impression that perhaps has been obtained from this session is that, although the telecoms sector is interested in fraud being committed in its channels, it is not incentivised to do very much about it, apart from perhaps reputationally, Alex, where you say that BT does not want to help people to make money from crime.

In terms of policy recommendation, is there also perhaps a need to incentivise membership of the strategic board or whatever to make sure that the telecoms industry is front and centre in tackling fraud, in the way that the banks now have to be? Alex, would you agree with that?

Alex Towers: I would not say that we are not incentivised at the minute. I absolutely think there is more to do, and of course there is a reputational issue. We have 20 million customers, and we want to protect them and make sure that they have a good experience. This is clearly damaging that, and we care fundamentally about that and about fixing it, hence lots of the investment that we have put in. I think it is fair to say that we have been too slow, and in the last couple of years we have accelerated quite a lot.

The question now is about other incentives, absolutely, and whether there is a bit of regulatory tightening up and levelling of the playing field. I think there probably is, and there is a role for Ofcom there. The political dimension is good now. There is a clear focus on this.

We do a huge amount with the banks, it has to be said. We have not talked enormously about the technical ins and outs of that, but of course they are our customers as well. It is very important to us that we have the best possible relationships with them, and ways of trying to protect them and their customers, because all of that matters equally. We are not just sitting on the sidelines and saying that it is a problem. We have huge amounts of ongoing in-the-weeds activity with them. We are piloting all sorts of new tech and ways of doing things, precisely because it is a shared problem. I do not think we lack incentives, but perhaps there should be a bit of tightening around the edges, yes.

The Chair: Hamish, do you have anything to add?

Hamish MacLeod: I have nothing particularly to add to what Alex has said.

On the policy recommendation question, I have probably already said it. We would be very happy if the head of the NECC got his way and a greater proportion of police funds was spent on this area so that more of the packages we produce for prosecution go the whole nine yards.

The Chair: Thank you both very much indeed for your time. I know preparing for a Select Committee takes some considerable time and we are very grateful to you both for being here this morning. It has been very helpful. Thank you all.