Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 7 April 2022

9.25 am

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Lord Allan of Hallam; Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; 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. 10 Heard in Public Questions 92 - 106

Examination of witnesses

Joe Lycett and Michelle Cox.

Q92 **The Chair:** Good morning and welcome to this evidence session of the House of Lords 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.

We are absolutely delighted this morning to be joined by Joe Lycett, who probably needs no introduction but is a comedian and television presenter, and Michelle Cox, who is a producer at Rumpus Media. Thank you both very much indeed for making yourselves available for this first hybrid session of this Select Committee.

We would like to explore the stories that you have been working on relating to fraud and scams and the people who have come to you. What types of frauds and scams is your programme contacted about most? How many people do you have coming to you? Is it lots? Is it a question of people being stimulated because of what they see on television and thinking, "That is a similar experience to one that I have had"?

Joe Lycett: As a general note, all the scams that we deal with or that we see generally follow a similar pattern, which is somebody pretending to be someone or something that they are not in order to get money out of

someone, in its most basic form. We seem to get a lot of email scams in particular, such as people pretending to be HMRC and talking about giving people tax rebates, and that kind of thing. We also see a lot of banking fraud; people pretending to be banks. They can also come in the form of messages from text messages and WhatsApp, and obviously phone calls.

There are other official bodies that people pretend to be. Quite often it will be across multiple platforms. People will get a message, an email or whatever, and a follow-up phone call or text messages, that kind of things. We had a big story about the dark web on one of the series and how a lot of passwords end up on the dark web on what they call a "sucker list", which is a nice title for it. Essentially, the scammers will find your password for your email and hide in it, watch your emails come in—they can do that sometimes for months on end—wait until some financial transaction is coming up and then swoop in with what looks like a legitimate email account, but they have changed the banking details and then they take the money. People have lost millions thinking they are buying properties and actually they have just sent money straight to scammers.

We have also seen a lot of get-rich-quick schemes. These are often on social media. You often see YouTube adverts for people who will claim to help you solve your financial woes but have nothing really to offer there and take a lot of money for the privilege. Also on social media are a lot of scam products. Unfortunately a lot of influencers get caught up in promoting products that do not work or sometimes do not even exist. We have seen a bit of that.

This is not a traditional scam, but particularly in the last series we had a lot of messages about the cladding crisis and people being messed around by the fact that their properties are no longer worth anything, essentially.

There is also romance fraud. We have not dealt with that on the show, but we have heard quite a lot about it. I do not know if anyone has seen "The Tinder Swindler". It is a classic case of someone looping people into a romantic relationship and then taking money from them gradually.

Michelle Cox: There are quite a lot of multi-platform, middleman platforms that we get irritated by—for example, places where you might want to purchase a dog, and the particular platform says, "All we do is host adverts for people who sell dogs". They do no vetting whatever, and people can end up unwittingly buying a puppy that is sick.

We had that sort of thing with Airbnb a few times. We first looked at it about five years ago. It was astounding how the platforms would wash their hands of any responsibility because they did not do any vetting or checks on people hosting properties. They do now, but they did not then. We found one property in Hyde Park that was worth £23 million. Somebody had stolen the pictures from the sales brochure when that property was available, put them on Airbnb and pretended that it was

their own. People were paying money to stay in this incredible penthouse, but of course it was all fake and there was no possibility of getting there. Even basic things were faked. The host of that particular property was a 21 year-old guy who had a dodgy photograph for his profile picture. Clearly that does not add up, but people do not necessarily connect the dots in that way. That is something else that we see quite a lot of.

Joe Lycett: We managed to list all the offices of Airbnb on Airbnb and get people to rent them. I think we put the person who was renting the property as Brian Chesky, the CEO of Airbnb, and they did not check it, they did not stop it. We turned up to their offices with the paperwork saying, "We have rented this property on Airbnb", and they did not like to see us. They did not let us in.

The Chair: How strange. We will come on to victims and fraudsters in a moment. First, out of interest, have you seen anything on crypto and Covid-19—you know, fake things like paying for PCR tests? We have had some evidence like that, sadly, with the Ukraine situation. There are always fraudsters who will take advantage by setting up fake donation sites and that sort of thing. Have you seen anything like that?

Joe Lycett: I will pass over to Michelle on this one. We have not dealt with any of them on the programme, but I am sure we have had stuff in the email account.

Michelle Cox: Yes, we have. Every time there is an opportunity to exploit a situation, people will start to send out messages. There was a recent announcement about Ukraine charitable funds and how it is better to give to the official 15 set-ups. We always get information about that sort of thing, but it is all from the same seed, isn't it? It is all basically people buying these sucker lists from the dark web and mass texting or messaging via email hundreds of thousands of people, and just one of them needs to fall for it and the fraudsters have their money. We did not realise how you can buy bits of kit that can call or send messages to hundreds and hundreds of phone numbers from sucker lists at the same time. It always baffled me. How could you sit there and send a million messages? Well, the kit exists and is being used for these kinds of nefarious purposes.

The Chair: That is very awful.

Q93 **Viscount Colville of Culross:** You have talked about online scams, and we have heard a lot about how they are on the increase. Why do you think they are so widespread? Do you think part of the problem is that the scamsters are not afraid of being prosecuted? Joe, could you answer that?

Joe Lycett: Yes, of course, Viscount. I do not know if I have ever met a viscount before.

Viscount Colville of Culross: That is very thrilling for you. I am so pleased. A first this morning. I have worked in television for most of my life as well.

Joe Lycett: True?

Viscount Colville of Culross: Yes.

Joe Lycett: It is so widespread because it is a numbers game, as Michelle just said. You can set up systems that send out hundreds of messages a second, and unfortunately there will always be somebody who is caught out by them, whether they are just vulnerable to it, they do not understand that it is fake, whatever it is, so it is a profitable business model at its most cynical. It is anonymous a lot of the time, so people are likely to not be caught. It is very hard to know who is responsible for making the calls or the texts, and often they are from overseas. We know that there are farms of scammers, people based abroad, who do this all the time and very successfully. I think it is unfortunately just the nature of the ability to get in contact with people across different platforms—social media, texts and all the other things—that makes it a viable business model.

We were talking about this yesterday. We also think that it is potentially a bit too easy to open a bank account. Without going into too much detail, I managed to open a bank account in someone else's name, with their permission, and that felt concerning to me—that you could open accounts without too many questions being asked. It is quite easy to funnel money in that way.

Michelle Cox: Depending on the type of scam, the anonymous ones are almost impossible to stop. A lot of them rely on call centres in different parts of the world from where they are able to contact us. There was a good programme the other day called "Scam Interceptors", which looked at how it happened and tried to intercept the calls before people parted with money. It is so anonymous. People are using fake phones, fake names, fake photos; it is impossible to manage it. That is why I think we should be pointing the finger at some of the platforms that could be doing more, because they have a responsibility.

We also look at individuals, such as lettings agents who are scammy or smaller companies that you can take more direct action to. However, it is difficult to police the big scams, isn't it?

Joe Lycett: Yes.

Q94 **Viscount Colville of Culross:** Michelle, do you think part of the problem is that the police have it as too-low a priority; that it is volume but in many cases involves a small amount of money and possibly from outside their police areas?

Michelle Cox: Yes. People can lose different amounts of money, but for the smaller amounts it is just chalked up to experience. Also, I think people feel quite ashamed when they fall for scams and probably do not always want to come forward and explain what has happened, so a lot of it goes unreported, which means that it is even easier for people to get away with it.

Viscount Colville of Culross: Even when it is reported, do you find that there is no action by the authorities, particularly the police, to do something about the scammers?

Michelle Cox: Yes. All the cases that we have been involved in are ones that have gone to all the different authorities but have had no success. We are the last resort of the A team.

Joe Lycett: There are cases where the scammers pretend to be the police themselves. We had one that was really awful. A woman was contacted by the "police", who said that they believed that her bank was giving out fraudulent notes and they asked her to take out, I think, £15,000 from her bank in twenties so that they could check the notes. Then somebody turned up at the house, saying that he was from the police. She was an older woman who had just lost her husband, who had been in control of the finances, and she handed over the money. When she contacted the police to find out how the investigation was going, they said that unfortunately because she had handed the money over there was nothing that they could do.

Michelle Cox: And how do you trace that person? It was just an anonymous phone call.

Viscount Colville of Culross: Do you think the police could do more to deal with problems like that? That is a really bad story, but it is replicated across the country.

Joe Lycett: I do not know what more they could do in that scenario, because it is so difficult to trace that person. Where do you get the compensation from? Do you get it from the bank for allowing that to happen? That is a tricky one to answer. I suppose you could hope that the police would try to trace where the number came from originally and go through that route, but I also suppose that is why they do not investigate as much as maybe they could or should: because they know that ultimately they will not get a result.

Viscount Colville of Culross: Yes. Okay. Thanks.

Q95 **Lord Vaux of Harrowden:** There are situations where you have identified fraudsters and confronted them, but the police have not. Why are you able to do this and they are not?

Joe Lycett: Resources, I am guessing. I do not know. Our show is to find these people and confront them. It also extends to the platforms, which do have a lot of resources. There is a lot of money behind them. Take Airbnb and the pet websites. We have got pretty close to confronting these scammers, and sometimes have confronted them, because that is what our show does, I suppose. I am guessing that the police have a lot of things on their plate.

The Chair: It is an attitude of mind, is it not? You want there to be a conclusion for the programme, and, for the victim, getting to confront someone is important.

Joe Lycett: Yes, but also we get so many messages that we do not deal with 99% of them, I would say. We do not have the resources to deal with all of them either. The volume is enormous.

Lord Young of Cookham: Joe, can I go back to something you said right at the beginning about the sucker list—the passwords of people that have been stolen and that are on the dark web? Would it not be possible for the police, the fraud agencies, to get hold of that sucker list, if it is available on the dark web, and do something to try to protect the people on the list from further scams?

Joe Lycett: Potentially, I suppose, yes. I do not know exactly. I am not someone who spends a lot of time on the dark web. I do not know exactly where you find the lists, but I think that once they have been procured they are relatively easy to find. I do not know if you buy them or whether they are just openly available, but I suppose that once they are identified, informing people that their passwords have been compromised would be quite a simple thing to do. You would have the email address. The problem is that if the scammers are in your email account, if they clocked an email like that coming in they would just delete it, so it may not be as simple as it might sound. Do you know more about how the sucker list, Michelle?

Michelle Cox: I do not know masses about it, but I do know that you can buy people's data for about 20p per person and that it can have loads of information, such as their telephone number and addresses, or it can just have partial information but even that tiny little nugget can be enough for a fraudster to go ahead and commit their scam.

We did do some research. We bought a sucker list with all the compliance and legal parameters in place and tried to contact a lot of the people on it to inform them that their data was for sale. We could not get hold of, I think, 80% of the people on the list, but we spoke to a couple of people, who were appreciative of that. We told them that they needed to change their passwords and gave them some information about how to protect themselves in the future. The dark web is so awash with people's personal data, I think it would be very difficult to stop it being sold, particularly as it is so cheap, but where there is a will, there is a way.

The Chair: Absolutely. Thank you.

Q96 **Lord Sandhurst:** Joe, your programme often criticises big business for its rather lacklustre response to fraud when you confront them with a fraud that has happened. I do not want to go into particular types of business, because that would lead you into an answer, but having set the ground, are there any particular sectors that you think could do more and are not doing enough to stop fraud and help victims? That is the first question. Secondly, when you have confronted big outfits, how have they responded?

Joe Lycett: To the first point, the biggest sector that we think could do better—we have mentioned it already—is the platforms. By that I mean

your social media platforms and businesses like Airbnb, but there are lots of businesses like that which are offering an intermediary to a service. They have definitely improved, but a lot of the time they go, "It's nothing to do with us. We've just offered the platform on which you meet and find these businesses, and if you get scammed it's nothing to do with us". Airbnb has a big thing on their website where they say that if you pay off the platform, there is nothing that they can do. That is a big thing: making sure that when you book something on one of these platforms, you use their official payment systems.

In the first series we did a story about banks and banking. In my observation, they have improved a lot since we started, but it is still at their discretion whether they refund their customers who have been scammed. A woman called Claire Leslie had been scammed out of a lot of money. She was with NatWest. She had essentially been told that there was nothing that the bank could do. I think their argument was that they cannot stop people pretending to be something that they are not. The scammers were very sophisticated in the way they did it. They managed to text her and it looked like the text was coming from NatWest. It was within the thread of texts that she had already had with NatWest, so she believed the whole thing to be legitimate. We decided that their argument, "We can't stop people pretending to be us", was not valid. I set up a Twitter profile for the head of RBS. His name has escaped me.

The Chair: Ross McEwan.

Joe Lycett: Ross McEwan. I pretended to be Ross McEwan for a few weeks, and then started tweeting slightly more erratic things as the weeks went on to illustrate that it has an effect on people and that it should be stopped, and it was stopped. In the end, NatWest refunded Claire Leslie the money she had lost and now there are improved things in place, but it still feels a little bit like it is up to the bank to decide, and if you get lucky, great. Precedents like the one we set with Claire Leslie help, I think, but it should not get to that point.

Lord Sandhurst: You have identified Airbnb. I do not want to name and shame particular platforms, but it would be useful to know what type of platform you have in mind. You can name one or two. I can visualise Airbnb. What other types of platforms are there that people use in volume?

Joe Lycett: We mentioned the pets one. We did a story on a platform called Pets4Homes. This was a big thing in lockdown: a lot of people wanting to get pets, feeling that they wanted a companion. Pets4Homes offers a service where they put you in touch with people who are breeding animals. As Michelle said, we found that some of the people on those platforms were breeding those animals illegally, smuggling them in and so on, and unfortunately often people would buy a puppy and the puppy would have illnesses that should be treated. In this country, we treat them if you buy them officially.

Lord Sandhurst: Is where we are going that you would like to see some

sort of obligation on the platforms to check the people who come on to them—in other words, the fraudsters?

Joe Lycett: Improved checks on those platforms seems to me to be a relatively simple thing to do, a reasonable request of these platforms and not something that is beyond their resources. These platforms are often making a lot of money simply because it is such an easy thing. Once they have set up the platform, they do not have to do too much afterwards, but I think they should be obliged to do more in that area. It could be similar with eBay and social media platforms as well, where they facilitate and watch. All those things should be better monitored.

The Chair: I do not want to pre-empt what my colleagues will ask, but what about the telecoms companies? Baroness Bowles, have I stolen your thunder?

Baroness Bowles of Berkhamsted: Partly.

The Chair: Go on, Baroness Bowles. Sorry. I have people in the room whispering "telecoms companies", so I thought I could not let that go.

Q97 **Baroness Bowles of Berkhamsted:** Have you done any research on the telecoms companies? They are the messengers for a lot of this. Do you think they could do more to intercept? You have mentioned dialling equipment dialling thousands of people. It is also used for many other very irritating things—"Do you want to claim some benefit?"—that are legitimately available. I accept that it is a technical question that you may not know the answer to, but could more be done on the sale of equipment, the models by which you can make these multiple calls, or indeed on the telecoms companies stopping them?

Joe Lycett: I do not know the technical side of it. It seemed mad to me that it was possible for somebody to text you from a number that is not their own. That seems to me to be something. I do not know how the technical side of these things works, but the ability to text you within the thread of texts that you already have from your bank so that it looks exactly like everything else—it is not coming from NatWest spelt wrong or whatever; it literally comes from the NatWest number—and you can ring the number back and it will send you directly to an official NatWest number that somehow the scammers have texted you from, seems ridiculous to me, but I do not know how that system works. Michelle, do you have more information?

Michelle Cox: I do not. Interestingly, we have not looked at the telecoms side and whether there is more that they could do. We will have to do it in our next series.

Baroness Bowles of Berkhamsted: It is fair to say that we have been less than impressed so far when we have asked them. They have the money and they are the carriers. So, yes, go poke around.

Michelle Cox: On the point about whether businesses or platforms could do more, we were talking about how Claire Leslie, the victim in the

banking scam, did get her money back, but people need to be able to advocate for themselves and know how to complain properly. If people do not know that, no matter what the bank's policy is on refunds, if they just say, "Can I have my money back, please?" and the bank says no, they have to know how to get the attention, who to write to and how to write to them. Companies will say, "Yes, we have refund policies and protection in place", but unless people know how to navigate those things, it is often very difficult for them to get their money back.

Baroness Bowles of Berkhamsted: Have you picked up any effect of the additional questions that banks ask, particularly when people are trying to pay somebody for the first time? It took me a very long time yesterday to make a legitimate payment to a new supplier. At one bank, I could not even get the payment loaded and had to go to another bank, and even that bank imposed a delay without warning. It is all very complicated. If a bank rings a person up and says, "This might be a scam", and you say, "No, I think not", the banks say they will take the compensation away. Have you come up against that?

Michelle Cox: Yes. A lot of those initiatives have crept in over the last year or so. I think they are very good, because they always make me stop and think about who I am paying. But, again, they will not stop everybody, and the scammers do not need everybody to make a payment; they just need a couple of people to fall for it. Again, I guess, it is a numbers thing.

Q98 **Lord Gilbert of Panteg:** My question is on that point of bank liability. Joe, you said that ultimately the banks decide who they will compensate, and people have to have a bit of a fight with them. What is the remedy for that? It seems to me that there are two remedies; either you say the banks shall compensate everybody—but that seems unreasonable if people have been totally negligent, have been warned and have gone ahead with a transaction anyway—or you put in place another body that decides on the basis of evidence and perhaps the vulnerability of the customer whether a bank has any liability and that there should be compensation.

Joe Lycett: That sounds reasonable to me; having a body in place that people can contact and which will fight their corner or at least will look at it as quickly as possible, and determine whether they have taken reasonable precautions with their money.

Lord Gilbert of Panteg: And make a decision that is binding on the bank?

Joe Lycett: I think so, yes. Otherwise a bank could just wriggle out of it, I suppose, couldn't they? I appreciate the banking sector, but I also feel that it has some pockets and it provides a service, so it should provide a service that is not likely to be used for fraud.

Lord Browne of Ladyton: You appear to have taken the bait about looking into how scammers can text you from numbers appearing to be

those of your bank. I just want to abuse my position by not asking a question but encouraging you to do that by just sharing with you the experience of many people I know, including myself. Scammers can telephone you in the same way, which is not a surprise, but the system works in such a way that when I phoned the legitimate number of, in my case, the bank's fraud team, I got the scammers. They had managed to hold on to the line. When you are looking into it, maybe you could look into that too. Thank you.

Joe Lycett: We were talking about this yesterday. The scammers do this thing now where they call you and ask you to ring the bank and they remain on the line and catch you out that way.

Michelle Cox: And you think you are going through. It is so clever.

The Chair: I suspect that, by the end of this, if you do not already have plenty of topics for your next series, and perhaps all our social media suggestions, you will have after this session. We move on to victims now, because you do work with people who ask for your assistance.

Q99 **Baroness Taylor of Bolton:** You give a lot of advice to people and you raise our awareness, but, alas, lots of people do fall victim. Can you say something about the impact on them? I think Michelle said earlier that people feel ashamed, on occasions, if they fall victim. It probably makes them feel gullible and not want to talk about it, and lots of cases are not reported. Some of the cases you have talked about have clearly had a very severe impact. Do you think we have the measure of that impact? The police are not taking on a lot of the smaller cases, but the impact will still be there. Is that what you are finding?

Joe Lycett: Yes. The impact of these things is endless and very hard to measure, but it ruins people's lives. People have lost their lives because of the depression and the shame that comes with being scammed in these ways. Unfortunately, suicide is sometimes a result of that shame and that feeling of helplessness. It is sort of indiscriminate in that it affects everyone regardless of age, gender, income, class and all of those things. It is something that anyone could fall victim to at any point and it could completely change the course of their lives.

There is a statistic that I found quite extraordinary, which is that one in five people aged 16 to 34 had been scammed in recent years, compared to 4% aged 55 and over, so it does seem to affect younger people more than the elderly. Anyone can be caught out by it and it can completely ruin your life. So, yes, that is why I do the show and I am very proud of the show. It can shine a light on the thing. It does it in a fun and light-hearted way, but at the core is a very serious thing, which is that people are being wronged on a massive scale by these fraudsters and scammers.

Baroness Taylor of Bolton: Does it also undermine confidence in the way Lord Browne was just talking about? Banks, or their information, is being used to trap people. How do we stop being paranoid and worried every time a bank does contact us or ask us something? We are

undermining structures that we are very dependent on—HMRC, banks and other bodies.

Joe Lycett: The effectiveness of those scammers is in finding those vulnerabilities. They find that company or institution that we take very seriously and we think, "Oh, this is serious. I need to deal with this". Unfortunately, it is such a big problem that you will never find all the scammers, but you can tackle it through education and making people aware of the very basic things that they can do to protect themselves, their privacy and their information. That will hopefully stave off a lot of these scams.

Q100 **Baroness Kingsmill:** You mentioned education. I want to ask two questions. First, you are playing an important role, to the extent of your audience, in educating and informing people about possible scams. However, it is a bit of a responsibility for one programme to take this sort of thing on. Do you have any suggestions as to how we could educate more? When I was an adviser to a bank, we had a programme of financial education, because, for example, a lot of people did not even know what a mortgage was. They thought it was like rent. It was astonishing that people were not as alert and aware as one thought they would be. Do you think there is an argument for a more formal form of education to help victims?

Joe Lycett: Yes.

Baroness Kingsmill: I cannot, for the moment, think what it could be. I wonder if you can.

Joe Lycett: Very simply, it would be more information in schools, not just about being scammed but maybe lessons in basic things like the difference between APR and AER, what is a mortgage, what is rent—all these financial things that I was not educated about when I was at school, and I am not sure there are classes in that even now.

In terms of scams, there are some really basic things, such as changing the privacy settings on your apps, never using the default settings on things like smart devices in your house. If you buy a wi-fi camera, always change the settings to make sure that the password is not the basic password. Then there are things such as reverse image search. This is something that Michelle and I were talking about yesterday and that we use a lot. We forget that people do not know about it. It is a very simple thing you can do. If you get a message from somebody and it has an image—let us say on their WhatsApp—you can take that image and put it into Google image search and it will look to see if that image has been used anywhere else. Often that will reveal that it has been used millions of times, because it is an image that a group of scammers has used elsewhere. If people have these basic tools and are taught about them in school, it will help.

Michelle Cox: In one of the series, Joe had a brilliant interaction with a classic email scammer saying that he had won millions of pounds and that he just had to transfer some money, and they sent a picture of

themselves on their deathbed. We looked at that picture on a reverse-image check and found that it had been used about 2 billion times. It was just an actress from a programme and the scammer had used the still. It is such a valuable tool.

I really do think that you need to teach people in schools, particularly because so many young people have tech in their hands and will be flooded with offers and information, on Instagram for instance, about amazing products that they need to buy, and they will not have the skillset to navigate between a genuine offer and a scam. Quite a few scams promise work. We see quite a lot of messages where you can sign up with an agency but you will not get any work. Learning how to protect your own information and knowing how to complain are two key pillars that should be taught at school.

Baroness Kingsmill: Earlier on in your testimony, you said that you deal with only a small percentage of the complaints that you get and did not look at about 90%, or you looked at them but did not use them in the programmes. What do you do with that 90%? Do you formally pass them on to the police? Is there a screening process, or do they go in the bin? What do you do with the 90% that you decide not to use?

Joe Lycett: I will leave that one to Michelle.

Michelle Cox: We have an amazing team of people who will sift through all the messages. Compliance-wise, we would only ever look at a particular scam that has affected a number of people, and once we have done all our journalism, to ensure that it is a legitimate story. Of the rest, if it is a particularly personal story, we might contact the person and go through some suggestions about where they can go for help, but we do not have the resources to respond to everybody.

Baroness Kingsmill: I appreciate that, but I wondered if you sent them to the police or anything like that.

Michelle Cox: Not as a matter of course, but where somebody had lost a lot of money, we would suggest that they go to the police, Action Fraud, the CAB or any of the organisations that might be able to support them. We often refer people to Trading Standards as well.

Baroness Kingsmill: It is a big responsibility, of course, because people share the most awful things that have happened to them with you. I just wondered if there was a formal way. You obviously cannot deal with them all but somebody else could. It is an interesting thought.

Joe Lycett: There is a bit of cross-pollination. Our show shares Michelle and quite a lot of the team with a lot of other productions, such as "Watchdog" and "Rogue Traders", where stories might not be suitable for our show because we are a light entertainment comedy show and some things are too dark or too serious for us, and those stories often find their way on to other programmes because of that. A story does not always just end with our show.

Q101 **Lord Allan of Hallam:** Michelle, you just mentioned Action Fraud. The official government advice is that people who are victims should go to Action Fraud and report it there, but lots of questions have been raised but how effective Action Fraud is. I am curious about your experience. You have a lot of people coming to you. Have many of them been to Action Fraud, and what is their experience of doing that before they come to super action fraud or however you would style yourselves?

Michelle Cox: I like that name. People have not always had the best experience, and likewise with the financial ombudsman; sometimes they have not got the results that they believe they are entitled to. The problem is so enormous and people have to be so tenacious to get a result that they give up, I think, whereas when we have the right case, a case that we feel will shine a light for a wider audience, we can keep going at it. When we get our rights of reply from companies, we rarely settle for the first one. We will interrogate them and go back and push to try to get a result that is fair. I do not quite know what an organisation like Action Fraud, which does loads of great work but must be so overwhelmed by cases, can do to improve how they deal with customers. But, yes, we certainly have had lots of people who have tried and exhausted other avenues of support.

Lord Vaux of Harrowden: I was struck by your comment about default privacy settings on kit and equipment. We obviously have lots of rules on electrical safety and things like that. Do you think we should be putting in rules on default settings so that they are set at the highest privacy settings when people buy them, and similarly for apps and that sort of thing?

Joe Lycett: That could be investigated. The problem is that smart devices often come with a default password that you have to know in order to change it to make it more secure, and I do not know how you would get round that, not being a technical person. I do not know if they could all come with unique passwords, that kind of thing, but it is often the cheaper stuff that does not adhere to any privacy things. Even changing a password is not enough for a lot of these things anyway, but yes, the quality of the products could definitely be improved upon.

Lord Sandhurst: It just occurred to me as you were speaking that a fairly simple device might be if the appliance you buy had a provision that said that you must change the password within seven days of first use or the machine will stop working. I do not know how practical that is. Is it something that could be explored?

Joe Lycett: Yes, absolutely. There are so many different types of devices, so whether you would notice that it had stopped working, your lights and so on, all that kind of thing, I do not know.

Lord Sandhurst: I was thinking of phones, tablets and PCs for a start, not fridges.

Michelle Cox: People do not realise that you have to change the default password. Whenever I have a discussion with someone about that they say," Oh, I didn't know you were supposed to change it". Step 1 in every instruction manual should be, "First, change the default password so you cannot be hacked". That seems like an obvious step.

Joe Lycett: However, with privacy settings on things it is sometimes hard to know what you have agreed to. We tracked somebody who was running a slightly dodgy company. They were a regular cycler and used a cycling app, and their privacy settings on the cycling app basically meant that anyone could see their routes, so we worked out how they got to work based on the way they used their cycling app. They just had not changed the privacy settings in that app. People are more trackable than they realise with some of these things.

The Chair: A lot of this, and a lot of what you see presumably, depends on human behaviour. I was struck by your comment about people tending to do what their banks or other people tell them. That is sort of hardwired into us, is it not? It is a bit like you do what the police or HMRC tell you. When you are talking to victims, how often do people say, "Well, it took ages for me to realise that this was a scam", or, "I just never thought that this would happen to me"?

Joe Lycett: Very often. People are so busy that they do not have a lot of time to interrogate these things. If something comes in, they might go, "Oh, I need to pay this bill", or whatever. People do not have the time. That is a very common thing.

The Chair: Michelle, does your team have to do quite a lot of counselling?

Joe Lycett: That should be a little sideshow, the counselling that comes afterwards. You were going to say something, Michelle.

Michelle Cox: I cannot remember. Sorry.

Q102 **Lord Browne of Ladyton:** This is probably the most open question you have been asked in this session. Joe, you have already told us that you have been surprised at how easy it was to open a bank account in somebody else's name, so I will generalise that. What has most surprised both or either of you about fraud and scams in the UK over the time you have been producing your excellent programme?

Joe Lycett: Thank you for the review. That is very nice, thank you.

Lord Browne of Ladyton: So you have to give me a good answer now.

Joe Lycett: I will try my best. The volume of scams really surprised me, the number of people who would get in touch, and the sophistication of the scams, the way they target the vulnerabilities of the people they are scamming. One of the things that I love about our show is that it attracts a younger audience; I have talked about the fact that 16 to 34 year-olds are more likely to be scammed than people who are older.

The 16 to 34 demographic is a demographic that we do very well in. We did a story about students and student accommodation, and how many students get caught out by scams because they are just so busy working on their studies—rather than anything else, I imagine—that they do not see these things coming. I am very proud that the show educates people in that area. I am also very grateful to Channel 4 for commissioning the show in the first place, because our show is not something that a commercial broadcaster would have approached. BBC said no to it. It is quite risky legally. Only Channel 4 would have commissioned the show, and it is an important part of the ecosystem of shows that help people being scammed. It is the volume and the sophistication that shocked me.

Michelle Cox: And the grooming, I would say. It is interesting, particularly with some of the longer scams, the romance frauds. Scammers will have a way of tapping into someone's vulnerability and just pecking away at it and using it, even over a very long period in some cases, to extract money. There is a ruthlessness. It is not a violent crime, so people tend to dismiss it as being less important than other crimes, but it is extremely exploitative, and the latest iteration always surprises me. I think that everybody must know and that nobody is going to fall for this, and then there is another twist to how scammers will lure you in. It is very scary.

Lord Browne of Ladyton: Thank you, and thank you for giving us yet another argument for not disturbing the current model of Channel 4.

The Chair: That is the headline from the session.

Q103 **Lord Vaux of Harrowden:** Following up on the rather surprising statistic that young people are more vulnerable to scamming than older people—I had always assumed it was the other way round—one of the problem areas is the way scammers get their money, which is often through money-laundering mules, who are often young people who have themselves been conned into allowing their bank accounts to be used. I do not know if you have looked into that at all in your show or if you have any thoughts about that area.

Joe Lycett: There are certain stories that are so heavy that we would not necessarily deal with them. We are a light entertainment comedy show on one arm and journalism on the other, so it is probably not the sort of thing that we would try to make light-hearted. There are other stories like that that we just could not deal with. But yes, that is a very common way of committing fraud. I do not know if you have worked on those sorts of things, Michelle, on your other programmes.

Michelle Cox: Yes, on money mules. There are particular banks that fraudsters seem to prefer using to target money mules. There are things that could be put in place to toughen that up. It is an interesting area. We have not covered it in the show but, again, next series—

The Chair: I think Lord Young was also going to raise the issue of mules.

Lord Young of Cookham: Lord Vaux has trumped me.

The Chair: All these Peers out-questioning each other.

Q104 **Baroness Taylor of Bolton:** In a sense, I am on the same issue. I was very surprised by what you said about 16 to 34 year-olds being so vulnerable, because we tend to think it is old fogeys who are not as tech acute who might be conned. It is surprising, because younger people are very tech savvy. Have you thought about doing anything with the universities or with the National Union of Students on the kinds of issues that come to them? All universities try to help students who get into difficulties—I declare an interest, because I chair one—but the National Union of Students must also see a lot of this. Is there any scope for exploring with them what might be necessary to help in that particular context?

Joe Lycett: There would be. We have done some stuff with a company in Cardiff—I do not want to get myself into trouble—

The Chair: My clerk has just reminded me that both of you are able to take advantage of parliamentary privilege, so you are able to name organisations in this session without fear of legal challenge. The QC here is nodding. If you wanted to name the bank, Michelle, that was rather too welcoming to mules and if you, Joe, wanted to name the company, you are welcome to do that.

Joe Lycett: Oh my God. I wish I had known that sooner. Gosh, the things I could say.

The Chair: Please carry on.

Joe Lycett: The company in question is CPS, which is based in Cardiff. It is probably one of the biggest, if not the biggest, providers of student accommodation. We have had so many stories about them, things they would say, like, "Oh, you've got to pay for this cleaning that's got to be done at the property", and the company that was doing the cleaning would be decided by CPS and owned by one of their family members. It is a real mess of a company and they were not thrilled to see us when we doorstepped them. We dealt with them. I am trying to think of other things that we have done with students at university.

Michelle Cox: Yes, the union was involved in that. We staged a raid outside and the student union helped us with that, and it turned out that it was not that difficult to get disgruntled students down there, was it?

Joe Lycett: No, it was a very popular event.

Michelle Cox: It was.

The Chair: Strange, that.

Joe Lycett: I do not think we have done anything specifically with students. We may well have done. We have done so many stories.

Michelle Cox: You said that we all know that young people are tech savvy, but I guess they do not have certain skill sets to protect

themselves. They are not finance savvy or fraud savvy. They can use the technology, but they still need to be taught how to protect themselves.

Q105 **Lord Allan of Hallam:** Before we lose your expertise, one of the issues we are interested in is the extent to which the fraud is committed by people in the UK or is cross-border, international fraud. You spend quite a lot of time tracking down the bad guys. That is one of the fascinating things about your work. Do you have a view? Does the trail often lead back to somebody in the UK? To what extent does it lead to people outside the UK?

Joe Lycett: We try to do only stories where we think we can effect some sort of change, so we will often focus only on stuff that we can change within the UK. Yes, there are lots of fraudsters abroad who commit fraud in the UK, but we have tracked down plenty who are committing fraud in the UK

The Chair: Michelle, this is almost your last opportunity. If you want to name the banks that are a little bit too friendly to money mule accounts, you are very welcome to do so. We would be delighted to hear that evidence. I will leave that with you.

Michelle Cox: Maybe off camera. I feel as if I need to triple-check before I say.

The Chair: We can always work out ways to make sure you get the benefit of parliamentary privilege. My clerk is whispering to me; written evidence. We can talk about that

Michelle Cox: It is some of the newer banks where there are not necessarily branches and it is all online.

The Chair: Very interesting.

Q106 **Lord Browne of Ladyton:** One striking thing about your evidence is your ability to create fake or assume other people's identities, including the chairman of a worldwide bank, and test their own businesses' resistance to fraud. Did you get any sense that any of these people you were dealing with, or any of these platforms, did this themselves? In security this is called red teaming; it is done all the time by people who take security seriously. Did you get any sense that they ever did anything like that?

Joe Lycett: I am sure they do. I just do not think that anyone else would approach it the way we did. Why would somebody pretend to be the head of a bank for that long and then tweet, "I've got a smelly bum bum"? At that point, the account started to get red-flagged.

Michelle Cox: They often have no sense of humour with it, do they? That is something. They really do not like it when you turn the tables on them.

Joe Lycett: Yes, and that is part of the effectiveness of the show. A lot of these companies do not want to be made to look silly, so that is why we try to make them look silly.

Michelle Cox: We have furious lawyers calling us. That is when we know—

The Chair: —that you have hit home.

Lord Browne of Ladyton: I am not trying to encourage them to compete with you. I am just wondering whether, in any of your interactions with them, they have said that they had good fraud protection because they had tested it for themselves—in probably a less entertaining fashion than you would do it—just to find out, "Can we fool ourselves?", when people are telling us that we are secure. Did they get somebody from outside to try to get in? Did you get any sense of that?

Michelle Cox: The first response to every legal letter is always, "We have fraud measures in place. Don't worry". It is only when we ratchet it up a notch and expose the flaws in their own systems that they take it seriously.

The Chair: I want to thank you both very much indeed for your time this morning. It has been very valuable, and on the basis that you probably tripled our audience I will just say for the benefit of anybody who might be watching that we are accepting written evidence. We would like to hear from all sorts of people involved in this, including, of course, those who have been victims of scams. You can find details of how to submit evidence via our Twitter account or on the House of Lords website.

Joe and Michelle, on behalf of the committee can I thank you very much indeed for your time this morning? It is much appreciated. I think you have had a few suggestions for what you might like to do in your next programme. We will look forward to seeing whether any of them translate to the screen at any point.

Joe Lycett: Thank you for having us.

Michelle Cox: Thank you very much.