HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Fraud, HC 125

Wednesday 22 November 2023

Ordered by the House of Commons to be published on 22 November 2023.

Watch the meeting

Members present: Dame Diana Johnson (Chair); Simon Fell; Tim Loughton; Alison Thewliss.

Questions 1-72

Witnesses

I: Cecilie Fjellhøy, Co-Founder, LoveSaid, and Anna Rowe, Founder, Catch The Catfish, and Co-Founder, LoveSaid.

II: John Kamoto, Policy Lead on Scams and Fraud, Age UK, Wayne Stevens, National Fraud Lead, Victim Support and Louise Baxter MBE, Head of the National Trading Standards Scams Team.

Written evidence from witnesses:

National Trading Standards Scams Team

Victim Support

Examination of witnesses

Witnesses: Cecilie Fjellhøy and Anna Rowe

Q1 **Chair:** Good morning and welcome to the Home Affairs Committee. This is our first session on the issue of fraud. We started our inquiry a few weeks ago and have lots of written evidence. This is the start of our formal hearings with witnesses. Today, we will concentrate on the impact on victims of fraud and the support that is available to them. We will start with our first panel. Please can you introduce yourselves for the record? Can you please give your name and tell us whether you are representing somebody or anything else you want to say about yourself? That would be helpful.

Cecilie Fjellhøy: I can start. My name is Cecilie Fjellhøy and I am the co-founder of the LoveSaid organisation, which is a fraud centre and think-tank that is helping romance fraud victims in particular. However, I am better known as one of the victims of the Tinder swindler. There was a famous Netflix documentary that came out in 2022 and after that I have been a spokesperson and activist, travelling around the world.

Anna Rowe: My name is Anna Rowe and I was the victim of a different kind of romance fraud back in 2015. I founded Catch The Catfish and later, when I met Cecilie, co-founded LoveSaid. I have been supporting victims of all kinds of romance fraud, including financial romance fraud, for the last six years. I deal with between 75 and 100 victims a week, so I get a really broad perspective of what is happening out there.

Q2 **Chair:** Thank you for that introduction; that is helpful. We are pleased you are with us today.

We have about 45 minutes for this part of the inquiry. I wonder, if it is not too difficult, whether you can both set out your story a little bit, just explain what happened to you and why you have then gone on to campaign in the way that you have and take the action that you have taken. Would that be all right?

Cecilie Fjellhøy: I had moved to the UK to do my master's degree in digital experience design and had just moved to London to finish up my master's thesis. I was on Tinder, which a lot of single people are, and I matched up with a man who was in London at the time, but I could see from his pictures that he was travelling around a lot. The next day, we met up and he looked like his pictures. He told me that his name was Simon Leviev and that he was a CEO of a big diamond company. He was travelling around the world signing and doing the last bit of the client work. We got into a relationship and he had this entire entourage around him, so when you were in his world, you were really in his world. It was the proper kind of romantic love that everyone wants to experience. I finally met my match, I felt—someone who adored me as much as I adored him.

He had this entire entourage, so the kind of romance fraud that I experienced afterwards was that I was really meeting him: he had personal assistants, I met his daughter, I met the baby's mother and I met friends of his. He had a bodyguard, and after a while he came into trouble where he had a lot of competitors who saw that he was doing well. He could not use his credit cards anymore because they could see where he was in the world by the spend on his card. He had a big security team that told him that.

At that point in time, he just asked me, "Do you have a credit card? If you do not, could you take up an Amex or something?" At that point in time, he was my boyfriend. I trusted him and I felt that if I could help him in the slightest—at that point, it was not a question of money. He had money, but he needed security. But as we all know when it comes to romance fraud, it did not stop. It just became worse, so I started to take up high consumer debt loans and was filling up this Amex card that I took out. They blocked that, and then I gave him my Mastercard. It was at the end of everything when I finally realised that he had taken over £200,000 from me. Those are high-interest loans, so it is an impossible debt to pay back.

I have to say that I did not recognise myself. It is so important to understand that I was a highly qualified woman. Not that you have to defend yourself, but I think it is so important to say that what you are actually going through is mental abuse. When I look back at the WhatsApp and the kinds of messages that he was sending me, I was working full time. Every single day the card was blocked, and I had to call and pretend that I was in Cape Town and say, "The card is blocked. Can you open it?" He even got me to send him documentation that I found out later was fake, so he was using my hands and my words to do his own doing. When everything was settled, everything was in my name. As we all know, he has gotten off scot-free. That is the story of the fraud. I don't know how much you wanted, but that is the fraud.

Q3 **Chair:** That is very helpful; thank you. I think most of us on the Committee, if not all of us, have actually watched the Netflix documentary. I am very sorry that happened to you. It is appalling, and you are very brave to speak out and to explain what happened, so thank you for being willing to do that.

Anna Rowe: I also met my abuser on Tinder after trying lots of other dating apps and having a successful relationship prior to that. He was claiming to be a divorced single father of three starting out in the dating scene after a failed marriage. He groomed me online, I now know, for three months before we actually met in person. We saw each other in person a couple of times a week for six months, and then the excuses started to come. Brexit had happened. He had told me while we were together that his mum had been diagnosed with cancer and was suffering with very ill health. I had a 6-foot lawyer stand in front of me crying, telling me that. This tells you how much they believe their own lies and how convincing they can be. After another five months, when his hold had come away from me, I started getting very paranoid about what was going on. We were still talking for the whole five months after this time, and I

went back online to see if he was playing around—playing the field—and whether that was why I had not seen him for such a long time. I very quickly found him online again and challenged him about it, and it was not long after that that I realised that he had been lying. I discovered that he was not who he said he was and that he had actually been living a double life.

When I had proof that there were other victims involved—although I did not know at the time who they were or how many there were—I went to the police and I was told, "So your boyfriend lied. What do you want us to do about it?" My reason for going to the police was that it became very apparent through my tracking him down. I did track him down to his real life and took that to the police. The reason for me doing that was because it had become very apparent that he was using dating apps to hunt for and target women for the purpose of sexual gratification as well as the kick of having control over people through the deception. The police would not do anything, and I went public with my story.

To this day, there are 17 of us that I know of just for that one man, including two aggressive rapes, a sexual assault and a handful of what is contentious sex by deception under consent law. It is this fight that I continue to have now. A case of eight to nine victims has been handed to CPS by the police, who eventually started investigating after two years of pushing, and the CPS has said that it does not reach the evidence threshold, so that is a continued fight.

After I went to the police, when I was turned away for two years, there was nowhere for me to go—same as Cecilie—nowhere for someone who had had an experience like mine. After being in therapy sessions, I was told to go and research narcissists and psychopaths. That is what finally opened my eyes to how this man had done what he did to me and had such a hold over me. I needed to put this information somewhere because I wanted other people to be able to find it, so I started my website, Catch The Catfish, and very quickly I started getting messages from people where it was obvious that sexual motivation was not the motivation, but financial fraud was. At that point, when they were sending me their messages from their scammers, I recognised the pattern and how they had been through this grooming process—love bombing, trauma bonding, the coercive control—to get a victim where the scammer or abuser wanted them to be to manipulate them for what they wanted.

I decided to learn a lot more about those particular kinds of scammers and I started building education and awareness websites across all social media. I now hang out in scammers' groups to keep up to date with their new scams. I met Cecilie—after six years I knew I needed to grow—and with LoveSaid we have now started to talk to police at conferences to update them about the process that happens within romance fraud to help them to help victims in a better way.

Q4 **Chair:** So things have improved with the police.

Anna Rowe: Within the five or six years that I have been doing this—whereas we started out with literally nothing—victims like Cecilie and I, after seeing therapists, would recognise the grooming process, but the authorities did not. We are very fortunate to have some academics that have taken on research now. Dr Elisabeth Carter is incredible. Cassandra Cross over in Australia is amazing. They have now put into academic research that the parallels between domestic violence and the grooming process that fraud victims go through is under the same umbrella as coercive control. Because that is now in academic research, authorities are starting to take notice.

While we have seen some brilliant steps and there are some improvements, we are really fortunate that after doing conferences the police are now coming to me when they have victims that need supporting. There are pockets of greatness. There are some really compassionate police, but unfortunately it is only a tiny percentage at the moment because the education and training is not out there.

Chair: I think we will probably have more questions on that. Simon Fell is next.

Q5 **Simon Fell:** Thank you both for coming and speaking up, and for being as brave as you are. I know how difficult that must be. Anna, I want to pick you up on something you said in your opening remarks. You said you were helping between 75 and 100 victims a week, and you have been doing this for five-ish years.

Anna Rowe: It's just gone six years now. That has built over time as my pages have become larger. I started off with barely anyone on my pages. Across social media I have probably got about 35,000 followers now. It is global, rather than just the UK. I don't turn anyone away just because they are in a different country. This crime is borderless, and so are the victims.

Q6 **Simon Fell:** I am just trying to get an idea of the scale of how many victims you have seen over that period.

Anna Rowe: It has to be into the thousands. That is just new victims that come to me. They all come to me on a different part of their journey. As we always say in the presentations that we put out there, every victim is unique, depending on so many factors. Whether the victim can accept quite quickly something to get them out of the fraud, or whether it can take months, it very much depends on the victim and where they are when they come to me. Also, it is not just victims; it is friends, family, carers. I get a lot of carers for disabled people who have realised that the person they care for is part of a fraud, too.

Q7 **Simon Fell:** I want to talk to you both about your experience of reporting the fraud once you had identified it and knew what was happening to you. Perhaps I could begin with you, Anna, because you mentioned this in your opening remarks. How did you find the police, and how has that response changed over time?

Anna Rowe: Their response to me was disbelief that I was even bothering them, if I'm honest. After the initial report, they just sent a PC with a domestic violence form, saying, "Do you think he is going to come and attack you?" That kind of tick-box effort, and that was it.

I then went public with my story, to start a petition, because I was having mixed reactions from lawyers to say that what he was doing was already covered under consent legislation, and others were saying it would not negate consent. I have become quite well regarded for understanding sex offences legislation now. I know it inside out because of what happened.

Every time I did something publicly, more victims came forward. Every time another victim came forward, I would go back to the police. Even at one point, when the response from this detective was, "Now that sounds more like rape." "Well, are you going to do something?" "No." That is the kind of response.

After two years, getting my information from the police, and going through some really badly redacted emails, they had left the mobile number on there of someone at the top of the police's chain of command—and I phoned it. It was because of him that my faith in the police was slightly restored.

He actually said, "If you are requesting that information, there is obviously something wrong." He was good enough to pencil me two hours out of his time with a specialist sex offences officer. He let me talk through what at that point was 14 victims. I said, "That doesn't sound like the email you were sent there, does it?" He said, "No. I'm horrified." He then opened an investigation; it took three years.

Q8 **Simon Fell:** I don't want to put words in your mouth but, in your experience, you would see it as a fragmented approach, with different areas of speciality across the UK.

Anna Rowe: Incredibly. I was told, with my case, that unfortunately, when the police are put into training they are stretched across lots of different areas, rather than having specialisms any more. The officers who are stretched across lots of areas do not get any in-depth knowledge, and are not able to think outside of the box, if you like. Those were the words of Emma Banks.

A lot of the victims who come to me won't even bother going to the police because the stigma around this is so huge. They also don't think that the police will do anything. Those that do are, more often than not, ridiculed and sent away. That is the reaction from some police forces. The other day, a victim went to them and they just said, "We don't do fraud here. Cyber-fraud is just reported to Action Fraud."

I went back to them and said, "But this is a victim in your jurisdiction." With that particular one, like Cecilie's, they knew who the person was. He was there in the local vicinity. I said, "Why are you not investigating that?" "Well, we just wait for it to be disseminated by Action Fraud. It is not something we would report."

Q9 **Simon Fell:** Unfortunately, it is all too common. Thank you. Cecilie, your case has been well documented.

Cecilie Fjellhøy: Not the story that is coming up now.

Simon Fell: I was going to ask about the case that is in the Netflix documentary. It has an international angle to it, as well, so you are not just challenged with reporting to UK police. You have international jurisdictions playing in there as well. Could you talk a little about what that is like, trying to get your story heard by law enforcement across multiple countries?

Cecilie Fjellhøy: I would love to talk about how I was received by UK police, though, if that is okay, because I didn't even mention how it was for me to report it. For me, it was horrendous. I had two special security agents from Amex who came to me and said that I should not report it to the UK police, because they were working on gathering a case. That was weird in itself, I thought. Then I received a death threat from my fraudster, which he sent to my work email. I then called the Amex person I had and said, "Now you need to go". He was trying to help me. When I then came to the police station—again, you meet a cold shoulder—luckily, I met an amazing woman. I was sitting there for four or five hours and gave all the evidence, and it was put into the domestic abuse category. Remember: I am not from the UK, so I do not know everything, such as who to contact and everything.

Victim Support then contacted me, which was amazing. They asked if I felt safe, because he knew my address here in the UK. At this point in time, we can laugh about his sayings, and for every action there will be a reaction, but remember that this was a big conspiracy. I owed a lot of money, and I had nine creditors going after me, while I had this man—I did not know what was going to happen to me. I was then most in contact with Amex and, first, with the police. I was going to go in as a witness. I went to report in May 2018, and in August 2018 I was going to go in as a witness. I heard a couple of days before that, "No, you don't need to come in as a witness". I never sent in any evidence to police, and they never even asked for it.

Throughout autumn, I was trying to give evidence and talk to them. The UK police would not speak to me at all. Suddenly it was at the CPS. At that point in time, I did not know what the CPS was, because I got no information from police. In April 2019, I got two police officers barging into my apartment with body cameras and a search warrant for my phone and laptop, because they had concluded that I had defrauded American Express with Simon Leviev without any evidence of that, after almost a year. I had been going about this, and I was like, "If you really thought that I was a criminal, why did you wait almost a year to get into crucial evidence?" Second of all, this was after the first "The Tinder Swindler" documentary had come out, so Simon Leviev was in hiding.

Simon Leviev was then imprisoned in Greece for two months. I tried to get information from the police, but I could not get any from them, because I

was a suspect. They took away my rights as a victim ever since it started. No information as a victim—think about that: there is the guy who made death threats against you, and you are not allowed to get any. I got an email saying that they had gone well beyond what I was entitled to, since I was viewed as a suspect. But even after, when they got my phone in April 2019, it was 1 September 2020 when they then dropped my case against Simon Leviev but dropped the case against me as well. Under no circumstances was I ever viewed as a victim by the UK police, and I am appalled that the UK police and European police did not manage to collaborate properly to get Simon Leviev and get him extradited.

These are the questions I have. I am saying: in the fraud community, if you cannot even get to a guy who is in jail and has a name, what are you going to do with the online fraudsters? I have worries now that people are going from drug trafficking to romance fraud because the sentence is lower. For me, it is fine; it is okay. I understand that romance fraud is not easy, but the timeline of this is horrendous to me. When I got the call when they dropped the case, they said they knew that what I had endured was worse, but they were hoping to get to him by going after me. What is that? I had to go through trauma; I had to go into questioning as a suspect with the police. I have asked for those cameras—for that evidence—because I was wondering; I was banging my head. To traumatise a victim who had gone through the worst like that—that is not how you treat a victim.

I have to say that this is what the fraudsters want. They want all the views to be on the victims and how awful we were, so they can go scot-free. Simon Leviev was laughing, I'm so sure, about the acts. He made a defamation lawsuit against me as well; I had to pick that up. I do not know if that was the taxpayers here, because that went from the Greek language to English. I had to pick that up from the Ministry of Justice. My old flat—when he used that, he was never questioned by the UK police and he was still free. For me, it is appalling police work, but I have to say that that is across Europe. The lack of collaboration has been appalling. I am still sitting here going to therapy because of the trauma I had to endure at the hands of the UK police—the Met police—in questioning and Operation Falcon.

Q10 **Simon Fell:** That is just an awful experience to have gone through, and I am very sorry that you had to. May I ask about—perhaps this question is one for you, Anna—your experience of cases like this? You have said you are seeing a huge number of international cases. Is this a common facet of them?

Anna Rowe: With Action Fraud the way it is, I get so many contradictions from forces that it's as if one hand doesn't know what the other is saying. I am really lucky with our connections now, especially with the amazing team up at City of London police. We know that when things are put into Action Fraud at the moment, it is very much dependent on whether the victim has managed to understand and know the exact criteria for the information needed by whoever at the NFIB then reads those reports to say, "Oh yes, that one is worth looking at and we'll chuck it back to a

police force." That, to me, is the overall impression that I am getting currently from police forces. Obviously, when it's overseas crimes with romance fraud, I understand it's really difficult. We know it's out of legal jurisdiction. We know the chances of justice for victims are tiny. But when it's in this country, I can't find an excuse for the behaviours of the police, other than they just can't be bothered. That is the impression that I get.

Q11 **Simon Fell:** I suppose the point I was trying to push you on there was whether Cecilie's experience of both being a victim and being treated as a criminal by the police is a common one—whether you see that recurring in cases.

Anna Rowe: Victims are scared. Sometimes they are threatened, especially within romance fraud where there is money laundering, because it's not always just money being extorted from romance fraud victims. It's sometimes money laundering, and they become part of a money laundering chain. I have had examples of victims who have been threatened: "Well, you're breaking the law." Even though they can't be complicit in that, because they didn't understand, they have been threatened with that kind of thing. So it is, unfortunately, not a unique experience.

Q12 **Simon Fell:** I have just a couple more questions, if that's okay. Cecilie, Amex were involved in your case, and other banks were as well. I am curious to hear your thoughts about whether they do enough—did enough in your case and are doing enough now—to alert potential victims that they may be being abused and that they may be being handled by someone else and manipulated by someone else. Do you think—clearly not in your case—that now there are better protections in place and they are heading in the right direction there?

Cecilie Fjellhøy: In my case, Amex was his favourite card, favourite bank, so you can just guess—I got a Platinum card, without any documentation, in my mail two days after. I wish that wasn't that easy. When I travel around now and talk about my story, no one understands why it wasn't stopped, because the bank should have seen the difference in spend. I had a very normal spend. I did not travel a lot, for example. It was only that I was in London but pretending I was in Cape Town. A lot of people have been saying, "Why didn't they have the measurements to check where you're calling from?" It's a very easy thing. I know that we are talking a lot about new technology and everything, but for me, it was the bare minimum that didn't work. There were also the fake documents that I sent in—suddenly I was "living in the US". I do not understand how they even got approved over there.

But as I say, the banks are quite powerful. If they don't want to answer you, they can just say, "We don't want to meet up with you." It is very difficult for me to see; what I have felt, though, when we talk with banks—we do webinars and talks—is this. They have very different processes and are very reluctant to open up about their internal processes, because of business. But this is crime. It's very weird for me that you're scared about lessening crime in your organisation and sharing

that with other banks. It falls a bit flat for me. But it seems that some are going to the police if they have someone vulnerable who is subjected to romance fraud—and we refuse to believe it. When Amex blocked my card, I sent a complaint email to them. How angry I was at them for blocking my card, and of course I was travelling around the world! That is how brainwashed we are. For me, I really want to know more about what exactly the processes are that different banks have. They need to open up. Some say that they contact the police to help us understand that we are being defrauded, but some say that by law and legislation—that is why I knew—they just have to send the money if someone wants them to.

The banks might be sure that old Gerda does not have a fiancé in Turkey—this is the fraud—but they feel that by law this is her money and that they should just let it go, which is insane to me, seen from a victim's angle. A crime is being committed against this human being—she is being mentally abused—and they are letting it happen. Even worse, it is a double-victimisation, and she will lose all her money as well—they know it, but feel that it is her money.

That is what has been most shocking to me. I wish we could put something in place so that, by law or something, the banks just have to stop the money. They say, "But people get so angry with us"—but let us be angry! We will be angry at them, but they need better training in the financial institutions, because a lot of them feel that they do not know what to say to break the spell to make us understand that we are being defrauded, but there are ways. As Anna was saying, take people on a journey. There are ways, and that is what I feel.

Q13 **Simon Fell:** My last question is about social media. You were both targeted by your abusers on Tinder. About 70-odd per cent of the fraud committed through the banking sector originates on social media platforms now. I am interested in your views about whether the platforms—such as Tinder, Meta or whatever it might be—are doing enough to put in place barriers to say, "We are seeing repeat activity here. This is something that you need to be concerned about. We need to educate you about this."

Anna Rowe: My experience of having worked on social media with victims for the past six years is that they are actively enabling it. It is not the case that they are doing anything; they are actively enabling it, including allowing the training groups for such scammers to be openly available on Facebook. Those Facebook groups have links to other groups, such as those on Telegram and WhatsApp. We can report even against verified profiles on Instagram or Facebook, for example, but they do not get removed.

AI for facial recognition is available. I could put in a familiar face, where there are 200 profiles, even with one name, using the same pictures. They are not removed. Every time I see a newspaper article in which a Meta spokesperson has said, "There are only between 7% and 14% fake profiles on our platforms," it makes me want to scream, because everyone who

does what I do knows that probably 50% of the profiles on social media are fake. They do nothing.

More, my account has just been disabled. One of my victim accounts on Instagram has just been disabled for fraud and deception. It has been targeted six times by scammers, so the scammers can report my profile and my profile gets removed. We can report the scammer profiles day to day.

Cecilie Fjellhøy: For us, it is the total difference. If you ask social media a question about this, they say, "It's so difficult. There's new technology. They're so quick," almost as if they are just giving up. But they suffer no losses for this. When we talk to the banking industry, which has losses with its reimbursement model, it says, "This is a big issue and we don't know what to do. We need help," but the social media companies are like, "Oh, sorry, guys. There's nothing to be done." That is when you meet the looking-down-on-you attitude—"Well, we have the laws and so much to go after," but for us, on the ground, when we report the profiles, it breaks us so much.

One of my friends had their account hacked. We know that is very lucrative because the hackers are holding a real account. I tried to report it—but it never gets removed. You feel like you are banging your head against the social media companies, and they are just saying, "Well, we're doing everything we can," and maybe putting up some posters about safe dating. They have the wrong priorities when it comes to this. To be fair as well, I feel that the companies get ad revenue for the amounts of active profiles—if we talk about the dating apps. That is one of my biggest things: why would they remove them? Why would they?

Q14 **Simon Fell:** They are earning money on the back of fraudsters. Sorry, I am taking loads of time, but I have a final question. In your particular case, there was an individual and, in the documentary, you say, "I saw him on Tinder and went to meet him. His face matched." He was the same person—the photos were the same. He was also doing the same thing to other women at the same time, so it was easy to identify that the individual who owned the account was the same individual who was committing the crime. Was your experience that, when that was reported to Tinder, it took no action?

Cecilie Fjellhøy: I don't know what Tinder actually did in my case. At that point, I had just deleted my Tinder. In my case, Tinder could not have done that much, but most romance fraud cases are purely online, so we have all the means to do so. In my case, to be fair, Simon Leviev was Simon Leviev out in the wild, so unfortunately that would be a much bigger issue.

Simon Fell: Thank you.

Q15 **Chair:** Are both these men still on Tinder?

Anna Rowe: Mine was, the summer before last.

Cecilie Fjellhøy: Mine is still defrauding. I was in a new documentary in Israel, where he is still defrauding, and I know about 10 people at a hospital in Germany. So even though he is not our problem any more, we have kind of given the problem to another country. That is what I am most sad about: I have done everything in my power, as one woman, and I put my heart and my entire private life out on the line. I do not know—maybe he is on another dating app.

Q16 **Chair:** But this one is on Tinder, Anna? This man?

Anna Rowe: During lockdown, without realising, he actually matched and kept trying to match with a past victim. I do not know whether he knew it was her, but she sent it to me. He was actively on there. He even sent another woman to me, because he was refusing to give her his name, and then he came clean that, if he gave her his name and she looked it up, she would find some information about him. He sent her to talk to me.

Q17 **Alison Thewliss:** It is really quite scary that he is still active in Israel and other places, abusing people. Do you think these types of abusers know that that is a tactic—that they can keep moving around the world and it will be more difficult for the police to catch them?

Cecilie Fjellhøy: Yes. Simon was in jail in Finland for two years, and I think he cooked up this new persona when he was in jail. He had three victims in Finland. I think he thought, "If I just stay in one country, that's bad news—let me just jump around." I even talked to the police here in the UK. They said that they were trying to get word from the Dutch police, and they said, "Well, that was in the media before we even saw it." Yes, it works for them. I do not understand why the collaboration is that bad. I think that is what is so sad for other fraud victims: if I cannot get justice, in a very high-profile case, what are the hopes? I want to be able to say that it works to never give up.

Q18 **Alison Thewliss:** It is absolutely wild that it is such a high-profile case and yet he is still able to move around, even with the convictions that he has.

Cecilie Fjellhøy: We are not naive, in that sense, but you think, "Okay, he had a judgment in Finland; he wasn't even supposed to be in the Schengen area." He was not even supposed to be able to be here, but he had some good fake passports. He had plenty of them.

Q19 **Alison Thewliss:** That is interesting—thank you. You talked a bit about Tinder not taking responsibility for this. Figures from TSB show that, from 2020 to 2022, 35% of romance frauds were on Facebook and Meta-type platforms, 24% were on Tinder, and 9% were on Plenty of Fish. Do you think that if the directors of these companies were liable, they would change their behaviour and change how seriously they take this?

Anna Rowe: Absolutely. This has been allowed to grow because of the lack of consequence. By not doing anything, they are actually benefiting from the situation as it stands. We keep hearing, "We remove so many before they are even made," but they are not doing the simplest on the front of it. We never see the evidence of that, but on the front of it, there

is nothing being done. I could go on any of those dating platforms now and, because I know so many of the faces that are used, I could collect 50 fake profiles within the space of 10 minutes.

Cecilie Fjellhøy: There was a case in Norway with a romance fraudster online. Tinder's spokesperson was interviewed and came up with a statement saying, "Well, people can just do reverse image searches themselves." I was a bit like, "You're a multi-billion-dollar company." How can you put that kind of responsibility into the hands of vulnerable people who are looking for love? We have very different tech competence, and we are not supposed to understand. For me, it fell so flat, and it felt very icky to see that coming from them.

Q20 **Alison Thewliss:** It certainly should not be on you, as a person using that platform, to do all that legwork and searching that you say you are doing, Anna.

Anna Rowe: Especially when they are making money off the back of those users. There is just no corporate responsibility behind user safety on these platforms. The dating platforms are a little bit more open to talking to us.

Cecilie Fjellhøy: They are. But I am hopeful that you will get Meta here, so they have to answer. We will see how truthful they will be. I wish that they would have to open up a bit more instead of just saying what they are doing, because I do not really trust that they are doing what they are saying they are doing. We would love to hear the discussions in their internal meetings when they look at, "What is safe dating?" They know that fraud is at the top here, and then there is what they are actually doing.

Q21 **Alison Thewliss:** We looked at this when I was on the Treasury Committee, thinking of economic crime. Certainly, it feels as though as very little has changed in the period between us looking at that then and us looking at this now.

Cecilie Fjellhøy: That has been our strongest impression, when it comes to romance fraud and taking down the person behind it and the abuse we are enduring. We have the numbers for it, such as how much money was spent, which is so sad. I think this is just the tip of the iceberg, because there is the shame. I know that I was the only victim who wanted to come forward here, because it is not much fun to sit here and talk about it.

Alison Thewliss: Absolutely. You are putting all your life out there.

Cecilie Fjellhøy: Yes. I am just thinking about the societal cost. I had sick leave, and I have had several others come up to me after talks dealing with house sales. We have suicides. It is so, so sad to see. We have no numbers for this, so it is difficult to get attention on the human cost of this.

Anna Rowe: That side is huge. In most cases, the emotional cost to victims far outweighs the financial loss, but in legislation there is nothing

to support the extreme emotional manipulation and coercion that a victim has been through.

Cecilie Fjellhøy: The police officer dropped my case because Simon Leviev had done company fraud here in the UK as well; he had defrauded a private jet company and luxury car company for £500,000. They upheld that case against Simon Leviev here, but they dropped mine because it was only £200,000. My heart just fell when I heard that, because it felt like what he did to me meant nothing. The death threats were not even mentioned again.

Q22 **Alison Thewliss:** Were you expected to pay all of that money back?

Cecilie Fjellhøy: Yes. In Norway, I was taken to court by four banks. I had to go through two trials where I was called naive and cunning. The banks said, "It is a tragic case, but it is not the banks' fault that Cecilie was defrauded." What can I do when the police say, "I'm so sorry"?

Alison Thewliss: That becomes difficult if there is no conviction against your abuser, as well.

Cecilie Fjellhøy: It is more about the traumatising things they do to you afterwards, where I feel like you are supposed to be protected. Maybe you raised your little hand and said, "Maybe the emails could have been stopped," and they said, "No, we have such great fraud routines." You feel—

Alison Thewliss: All over again.

Cecilie Fjellhøy: How I have been treated has just been really, really difficult. Especially when you go public when this type of thing, you really see the mean-spiritedness of how fraud victims are treated. I understand why people are ashamed and just want to forget.

Q23 **Alison Thewliss:** I will ask Anna a question. I have been aware of a few cases where there is also an international element—a visa element—to that as well. Perhaps somebody meets somebody online, and they get them a special visa to come to this country, and then they find that the person is quite emotionally abusive and economically abusive. Is that something that you pick up through victims as well?

Anna Rowe: Absolutely. There are a lot of cases of marriage fraud through these as well. I know a couple of people personally, who I have become friends with, where that has happened. It is a very common tactic with scammers after the scam. Once they have been challenged, the victim is in such a position, having had this intense relationship for so many months, that the thought of it ending leaves such a huge void. The scammers use that as what we call a follow-up scam, where they will then profess to have fallen in love with the victim, rue the scam, and say that it has not happened before. They will then say, "Is there any chance that we can be together if we start afresh? Can you possibly get me a visa to come and stay with you in your country?" That is an incredibly common ask, and obviously in some cases it will happen. I had one recently where someone

actually had the visa in this country but they were carrying out the romance fraud again.

Alison Thewliss: Thank you.

Q24 **Tim Loughton:** What struck me when I watched "The Tinder Swindler" was that it was a very sophisticated fraud and the victims—and the victim here—are pretty smart. This is probably going on for lots of other people in less sophisticated frauds who are not so savvy at dealing with them—yours is just the tip of a very large iceberg. What could be done? Is it down to more legislation? Is it down to better enforcement by the police, who do have the powers but are for some reason not using them, not taking it seriously, or not considering that this is a "proper crime" as such? Is it down to greater regulation of the social media companies because social media platforms are predominantly being utilised as the tool? Should there be greater regulation around banks asking more questions—obviously financial fraud is involved with romance fraud as well? Is it also down to better education and awareness, of which our inquiry is hopefully going to be a part—just as I am sure your Netflix series had a huge part in making people aware of it? Where would you start to change to try and eradicate this? Cecilie, would you like to go first?

Cecilie Fjellhøy: I really think that we need to change the stigma and there are many ways we can do that. One is with legislation. I really wish that the mental abuse and the coercive control that I was under would be put into the sentencing. I felt it was just about the money, and I felt like they said, "What he did to you as a person, we don't care about that. We don't care about the death threats or that you almost took your own life." Recognising what he did to me as a person, I think that would help the stigma and that people would realise, "Oh, okay. Romance fraud is mental abuse and coercive control." I think it is important for society to understand that. We have academic research that shows the similarities, so we have the foundation there already. I think that is one part.

Another part is that I really want the banks to start data sharing with one another and not to look at this as competition—it has been so weird to me, as I have said, but I think that is one part of it. Also, looking a bit more closely into some of the banks here—I do not know if that is a power of yours, but I feel like some of them are a bit looser. Some of the banks are saying this would be easily caught, and some of them are the ones who have been saying, "Why couldn't they see that you called from London?"—these very simple things that you think are already in place. Maybe you can take some of the others.

Anna Rowe: For me, our best approach to this is a holistic approach. You have got to look at it from a prevent point of view, as well as the right support being put in place, and education for all stakeholders whether that is the police, banks, and anyone who comes into contact with the victim. I feel there needs to be better regulation and consequence on any platform that is enabling these frauds. We had huge hopes for the online harms Bill that this was going to happen, but I feel from what I am hearing that it

has been watered down so much that it is not actually going to affect pushing them to be better at getting rid of these fake profiles and actually paying for employees to be there for victims rather than an automated system that fails every time when you are trying to get something sorted.

With law enforcement, we have started going out to speak to a few police forces, but everything that Cecilie and I do and have done for the last six years—these are things that we do in our own time and at our own expense. Romance fraud is an incredibly unique fraud, and it is by far the one that causes the furthest and the widest damage. I know from victims who have come to me—Cecilie gets them as well—that when they have this peer support, they will open up to us a lot more about the fraud that has happened to them, because they do not feel judged, and we have immediate understanding and empathy. There needs to be funding put in place because this is completely unique, and the support that is needed can be long-lasting.

Q25 **Tim Loughton:** I get that it is a holistic approach, but you have got to start somewhere. From a legislative point of view, we first look at whether laws need to be changed, and then whether the people we scrutinise—the police—need to better enforce them. It could be that there should be a greater role for the Victims' Commissioner, because you are victims, and this is a sophisticated form of victimisation.

I am struggling to see where the law could be changed. We have changed the law around coercive control, so now that is absolutely recognised as an offence—usually identified with domestic abuse. You do not have to present to police with cuts and bruises; there is another form of domestic abuse that is coercive control, and the mental damage that it does.

You have not really targeted the social media companies. Tinder is responsible for a lot. Other good dating sites are available, I'm sure. I am too old to use them, but my children tell me that they do. Should Tinder not have a duty of care, which may come as part of the online harms Act's responsibilities?

Anna Rowe: It absolutely should.

Q26 **Tim Loughton:** So that if somebody is doing these sorts of scams—much less serious than these—then they can be reported, and they should be taken down and banned. Or should you get to a stage where Tinder should have a duty of care to publicise known Tinder swindlers across its network as well? To make people aware that there are these people who have malign intent. That could be quite a lot of people if you are saying that 50% of profiles are fake, although only a small part of them are potentially up to no good.

Cecilie Fjellhøy: You have to remember that the fake profiles out there use innocent people's pictures, so they are victims themselves—in a sense. They are then maybe being subjected, on their social media, to people saying, "I've been in a relationship with you for six months", and they reply "No, I haven't".

Anna Rowe: The people whose pictures are stolen get abuse as well.

Cecilie Fjellhøy: We would love for known fake profile pictures to be more known, with the consent of the people whose pictures are being abused. That is what we are hoping to do, because it is lacking right now. People don't really know how to figure it out; I think a lot of people don't know what to do to find the fakes.

Q27 **Tim Loughton:** Are dating platforms approaching you for advice as to how they could make them better?

Cecilie Fjellhøy: We are finally in talks with them.

Anna Rowe: Tinder and Bumble.

Cecilie Fjellhøy: We are in talks with Tinder and Bumble. We are hopefully going to have an internal talk with Bumble soon, where we can present a bit of the data that Anna has—we can talk a bit more about that—because we want some answers. But, you know, again, it is business. We do not really understand the work they are doing, and what we are seeing on the ground, but we are there to co-operate with them; we do not want to point fingers and say, "You are the big baddie". We know that the people on the ground who we are speaking to are not the issue. There are bigger targets: KPIs and the return on investments, so I know it is difficult.

Anna Rowe: It is frustrating for us. Where I have been working on the ground, I get to see all the new trends that are coming in and the new pictures that are being used. There is such a wealth of data that they could easily utilise to make their platforms safer, that they have to choose to do that—or be forced to. It is incredibly frustrating.

Cecilie Fjellhøy: You can easily go into any Facebook group about dating and see plenty of people posting pictures, "Is this the real one?" Or people have been saying that they contacted the person with the real picture saying, "This happens all the time on Tinder." That is my issue. A picture gets reported, but then it is back on, so this poor woman, or man—whose pictures are being used in this crime—is then left feeling hopeless, because they are trying to get them down.

Anna Rowe: As part of my awareness, I use those pictures—the ones that are used all the time in the frauds. When victims come to me, or I know the very well-used pictures, these are what I post on my pages, because they then show on reverse searches and bring people to me. We can then give them the proper support that they need. It reduces revictimisation, which is huge, because they know that they have got a specific place with an open door to come back to when something else feels uncomfortable, and you can help to guide them through that, and educate them, so that we don't then get revictimisation, which is the issue we've got.

We have got some amazing places—Victim Support and Age UK. The latest campaign that has just come out from National Trading Standards, about

coercive control in financial fraud, is the best that I have seen. There are also some really dire campaigns that have been put out that are patronising to victims and make light of what is a really, really awful fraud and serious crime.

Q28 **Chair:** I just want to be clear. We are talking about individuals who are going on these dating apps in particular. Behind it, are there serious organised criminal groups as well? You've got individuals who are just one man, as in your case, but then you have got the serious organised crime.

Anna Rowe: Yes. We have got one person—

Cecilie Fjellhøy: Mine wasn't just one person, though.

Anna Rowe: Yes. But he presents himself—

Cecilie Fjellhøy: A small conspiracy, but we have bigger organised crime groups.

Anna Rowe: Mine was exactly the same process without money; yours was the process with money. And then we go into the global organised crime, which originates out of west Africa, with the authorities—these are very, very well-known. Those victims hardly ever see justice and they need support, because whatever one of those groups you fall into, the emotional damage is the same.

Cecilie Fjellhøy: We are seeing a new trend, which maybe you have seen in the papers, with both investment fraud and romance fraud gathered together as well. What we have heard is that, when it comes to organised crime, it is taken up another level, as well.

Anna Rowe: It's called "pig butchering". That's coming out of China. It's such a vile name; I don't know if we should be using it.

Cecilie Fjellhøy: I did not want to say.

Q29 **Chair:** Out of where, did you say?

Anna Rowe: That's coming out of China. They have collaborated with their criminal friends and we've got what used to be just investment fraud coming out of China but it is now combined with romance fraud to create pig butchering. Victims will go through having that relationship built for a long time and then they will be introduced to investment trading platforms; the majority of those are crypto. All of it is set up—"catfishing", as it's known.

The pig butchering is really harsh, because they are sent through, getting returns on their money for a long period of time, until they pass over the largest amount of money, and then they're gone. It's really horrible.

Cecilie Fjellhøy: The difference between my case, where money was—"Oh, I have an emergency", which has been the more common romance fraud. This is like, "You're doing this for yourself, you know—you're

making money for yourself. I just want to take care of you", in a sense. It's just such a horrible way. But they had to come up with something new, you know, and they are—

Anna Rowe: It is constantly evolving.

Q30 **Chair:** We are coming to the end of this part of the session. However, I just wondered whether you could just say a little bit more, particularly about the involvement of the police, because we have just been talking about the international perspective. Why is it that police forces are not sharing that information? Have you got any sense of why the information about either what is going on in particular countries or individuals who are travelling around is not being shared?

Anna Rowe: It's like keeping their little gems secret and in a box.

Cecilie Fjellhøy: I really think that fraud just has not been viewed as—it's almost like a victimless crime, compared with other priorities. And I think the police—we know that it is not easy for them to think about it. If you think about murders and domestic abuse and everything else they have to deal with, I just think it's been—and then I know as well that, when I've been talking just in general: they are all humans. Again—"Why are they still falling for this?"

I just think it is easier for them not to take it as seriously as other things, because we then don't have the numbers of the human cost of this. Then it's just like, "Oh, it's just money loss. They'll figure it out." But there's a lot of hurt behind it. It is training—making them understand what this actually is. Because I think the issue with fraud and scams and whatever, it comes exactly just from phishing—just clicking a link, or ordering something. And it leads to the devastation. I had to make myself bankrupt here in the UK—it is like this for life for me, and for everybody. It is a difficult thing for police to understand sometimes.

Anna Rowe: What is heartening is that when we do our presentations and I present to police who are not aware of the lengths that scammers go to—ours were in person, but when it is only online, they go even further to back up the lies to make sure the victim is completely beholden to them—when the police see all the things that scammers do, they actually start to understand more what the victim has been through and the sophistication of the crime. AI is a really huge part of that moving forward. I have already seen AI being used in deepfakes. We have moved from when scammers would use saved video of the person they were using and have two devices, one facing the other, so that on a video call, for example, the victim would be able to see who they thought they were talking to. Because it's saved video, they would sometimes do voiceovers on them. Now we have moved to deepfakes, which are far more convincing.

Cecilie Fjellhøy: It's so scary.

Anna Rowe: I am now getting AI voice cloning—a victim has managed to send me the first one to listen to, and I was shocked at how good it was. I could pick up a few nuances because I knew what I was looking for, but it

was enough for the victim, who had no idea that that technology existed, to believe and send money.

Chair: Thank you so much for coming to give evidence this morning, and for being so brave and willing to be so open about what happened to you. We really respect that. We are keen to carry on with our inquiry and raise some of the issues that you have talked about so eloquently this morning. We thank you again for your time and wish you all the very best. We will move on to our second panel.

Examination of witnesses

Witnesses: John Kamoto, Wayne Stevens and Louise Baxter

Q31 **Chair:** Good morning and welcome to our second panel. I am sorry for keeping you waiting. We just heard some very distressing and upsetting evidence from victims of fraud— I think you were in the room for some of it. Would you please introduce yourselves?

John Kamoto: My name is John Kamoto. I am the policy lead on scams and fraud at Age UK.

Wayne Stevens: Good morning, everyone. My name is Wayne Stevens. I am the fraud lead at the national charity Victim Support.

Louise Baxter: I am Louise Baxter. I am the head of the National Trading Standards scams team.

Q32 **Chair:** Thank you. We are very pleased to have you in front of us. Today we are focusing on victims, the effect on them and the impact on their lives. To start off, could you give us a flavour of some of the cases you are dealing with and the effect they have on individuals?

Wayne Stevens: With more than 3.3 million frauds last year, they cover a huge range of different sorts of incidents and affect significant numbers of people. There is a full range of impacts: from minor inconvenience, anger, annoyance, embarrassment and shame, to much more severe harmful effects, including physical ill health and people feeling unable to go to work or to study, through to self-harm and suicide.

I would like to give you an example from one of the people we have been working with recently, Alison. She met someone online, initially, and they struck up a relationship. He moved in with her and they lived together for 18 months. Over that period, within the context of their relationship, she was persuaded to lend money to invest in his business. She lent in excess of £200,000 over a prolonged period. When she asked for the money to be returned to facilitate a house purchase, he was unable to do that. He left, and she realised that she had been defrauded. She went to the police, and the police said, "This is a civil matter between you and your partner." She went to her bank and had a similar response: "This is a civil matter, not fraud."

She was absolutely devastated. She could not move house, because she couldn't purchase the house that she was intending to buy. She told us, "He knew how to mash my mind, how to isolate me, how to charm, coerce and manipulate…And with his repeated failures to pay on the promised dates, he brought me to the point of nervous exhaustion, unable any longer to see logic…I can barely afford my rent on the tiny roof over my head. I moved out of my other place last month because I couldn't afford it any longer…I have had to sell most of my furniture…I am on the council waiting list"—for housing—"despite having been a property owner and mortgage-free for years…I am terrified of the prospect of being an older person, alone, in years to come, struggling financially…I am traumatised by what he did to me…He robbed me of everything I worked so hard for…including my zest for life."

Alison is not her real name, but her story is very common. The impacts vary, and it is not all about the size of the loss of money, either.

Q33 **Chair:** Thank you for that example. It is particularly harrowing. John, would you like to give us some examples of what happens to a victim?

John Kamoto: For older people, the impact can be quite far-reaching and can also affect the whole family. As Wayne mentioned, there are the personal, emotional and social consequences of being scammed, and there is also the fear of being scammed. There is loss of trust in the local community or just in people in general, and people's confidence evaporates. In some cases, a person's independence can be questioned—for example, their family might think that their mental capacity is declining and that they might need to get a lasting power of attorney to take control of financial matters. For older people, the loss of independence is usually one of the biggest impacts.

Q34 **Chair:** Is there anything in particular? Are we mainly talking about financial fraud with older people? I always think of the example of someone who turns up at your door and says, "Your roof needs repairing. Give us £10,000," and then disappears and never repairs the roof.

John Kamoto: I guess that does happen, but since the pandemic, we have seen quite a lot of change, including people targeting older people by telephone—nuisance calls. That is the biggest worry among older people, especially because they might be alone at home. They are almost scared to be in their own homes, which is a frightening circumstance to be in. In a sense, the old ways in which older people were targeted, such as knocks on the door by "white van man", are not that common any more. Among other things, technology has changed the ways in which fraud is conducted. We definitely hear about people being targeted by telephone more than by a knock on the door.

Q35 **Chair:** Thank you. Louise?

Louise Baxter: My team tends to focus on older people, but we do scams awareness for everybody. We are aware of all the different sorts of scams.

You talked earlier about organised crime. The language that we use is really important. This is organised crime, and for these organised criminals, data is a really valuable commodity. They will groom individuals and then traffic their information from organised crime group to organised crime group. The more you respond, the more valuable you become as a commodity, and you are then targeted.

Although we talk about vulnerable consumers, we don't like to call people vulnerable, because vulnerability is about the situation or marketplace—it is about whatever you are doing or whatever is going on around you. With the cost of living crisis and everything that is going on with the instability of the world, we are all situationally vulnerable. They get you at a particular point when you are situationally vulnerable or having a period of mental ill health, and then, once you are in and you have responded, they will sell your details on. Then you will get bespoke targeting, depending on your particular affiliations or your visceral reflections—the sort of things that you want or that you are buying. It is really clever. I think scams is the wrong word. I am head of the scams team, so I'm not going to change that now, but it is the wrong word because it makes it sound trivial and it is not.

If we think about it from a consumer perspective, in 2015 a consumer called Joseph was neurodiverse—he had mild autism on the spectrum—and he received an email saying that he had been looking at inappropriate images on the internet and, if he didn't pay a £100 fine, he would go to prison. He took his own life. That was a literal interpretation of the email that he responded to. A 17-year-old took his own life because of his neurodiversity and his literal interpretation of that.

It is estimated that 15% of the population are neurodiverse. In the way they target you, they will know these things about you. If somebody puts on the internet—Facebook, for example—that "It's my son's birthday today. He has struggled with his life. We need to celebrate autism." They will know that and target that particular person because of those things. It is much cleverer—though that's not even a word—and much more intelligent than we give it credit for with these organised crime groups where it is targeted.

We can talk about a lady called Rebecca. She had 348 different direct debits going from her bank accounts to different criminal groups, who were selling her white goods protection policies, Sky warranty policies and Sky box protection policies. She did not even own a Sky box. She was 87 and had cognitive decline. She was on the telephone preference service. The criminals would use people who are on the TPS as an indication of a potential situation of vulnerability, and target those consumers. She lost £54,000 over three years. We were able to get that money back for her, but the criminals move and diversify so quickly.

As John said, during the pandemic we saw prolific mail scams moving to telephone scams. They would sell small amounts, such as £20—"We will protect your fridge, freezer, washing machine or Sky box. Oh, you need a call-blocking system on your telephone." We see it move from that to a

cold call of someone coming to spray your loft with foam insulation, "Because we are on the green agenda now and need to be energy efficient. Your bills are going to go up." That invalidates their mortgage and is a fire hazard.

They traffic their details to another company who come and offer to remove it for £5,000. It bounces and is constant. People are bombarded and they are socially isolated, so it is far easier for victims to be pushed into what is called a hot state, and being pushed into a situation where they may make decisions they would not have made had they not been pushed into that state, or had somebody else to talk to.

The criminals use tactics such as phoning you throughout the night for two weeks. They build on your insomnia, because we know that when we are tired or sleep deprived, we do not make rational decisions. This is vicious, disgusting, targeted crime. The criminals know far more about us than we probably do about ourselves.

Chair: Right, okay—I think we're all horrified by that.

Louise Baxter: Sorry!

Q36 **Chair:** You referred to an elderly lady who had all those direct debits going out of her account. How did that come to light? What happened that meant she was able to get help from you? Was it a family member?

Louise Baxter: No. We are running an operation that is looking in particular at these crimes. She came up as one of the people on our victims list, which the criminals nicely call suckers lists, which are the things that they sell. She came up and we went to speak to her to try to support her, to help to build our investigation and support the disruptive techniques we use to try to shut the criminals down from accessing UK systems. She is not alone; there is a load of them, unfortunately.

Q37 **Chair:** The other issue is that this is not just about the elderly, although they are vulnerable in many ways. This is about anybody. Younger people, people with professional backgrounds and well educated, are falling for these scams.

Louise Baxter: She was an ex-headteacher. She was really intelligent and not vulnerable on paper. You would not look at or talk to her and think she was vulnerable.

Q38 **Simon Fell:** I should declare an interest: Louise and I have worked together a lot in the past, so we know each other. Thank you everyone for joining us. I will pick up on your last point, Louise. This is the biggest crime in the UK by any measure, and it would seem that we are failing across the piece: the law enforcement response is not where it needs to be and there is not the money that is needed in the system. There are clearly a lot more victims out there than you, collectively, can deal with. What fixes this?

Louise Baxter: I think we start with language. That sounds very simple, but one of the recent studies we did showed that victims who report fraud

feel quite a lot of blame, shame and judgment from a law enforcement perspective, and I include myself in that statement; I hope that I am not one of those people, but trading standards is law enforcement. There is something around the language we use. We don't say, "You fell for a mugging," or, "You fell for a burglary," but in this case we place all the blame and shame on the victim, rather than on the criminal.

I heard the end of what Anna in the previous panel was saying in relation to peer-to-peer support to provide permission and acceptance that, first, we are all going to be targeted—because we all are—and secondly, that it is highly likely that, at some point, we may all respond; we may respond, depending on when we are targeted and what that situation is. We need to share our experiences and make it a conversation, like we do with mental health. It is not the same as mental health, but we weren't allowed to talk about mental health—we had to keep it a secret—and we are now allowed to talk about it, and that provides permission for other people to talk. That is how we are going to educate people, and I think that is our biggest arm of defence. We are not going to arrest our way out of this: it is—what?—2% or 1% of police resources, but it is 40% of all reported crime, and we reckon that between 15% and 30% of people report it.

We have to get better at sharing and talking about it, and making it all right for people to identify their own situational vulnerability. Nobody wants to say, "I'm vulnerable," because that word has negative connotations, but actually, situational vulnerability—"I was vulnerable at that particular time," or, "I didn't make the best decision because of what was going on around me"—might make it easier for people to self-identify. Saying that, that would be in a utopia, but I think it might help.

Wayne Stevens: To add to Louise's point, we think the public narratives around fraud need to change. We tend to talk about it as an individual crime that someone has fallen for or that someone has been naive about. Fraud is incredibly sophisticated and multi-layered, so we believe there should be better individually tailored information for customers, consumers and young people, to educate them on safe financial and digital inclusion, and also on safe online activity. There is a big education piece there, and we believe that anyone who has interaction with someone in a financial setting—a bank, building society, utilities company, social media company or whatever it may be—has a responsibility to try to educate people about the risk of fraud.

The second thing is greater industry focus on restricting the entry of bad actors into the system. The majority of fraud reports at the moment relate to authorised push payment. That is people like ourselves being deceived, coerced or cajoled into making payments. The banks can see those payments taking place on their balance books. We see examples of banks stepping in, suspending suspicious payments and making reports to law enforcement bodies, but we don't see enough of it, and often, it may only be after a second or third substantial out-of-profile transaction takes place that the banks step in.

Q39 **Chair:** Can you explain what that means, just so that we are all very clear

on it?

Wayne Stevens: It means that the banks see all the transactions on your current account, each and every week, and they build a pattern of data about you, so they have a sense of what an unusual transaction might look like. So if you were to suddenly make a payment to a virtual banking system outside the UK, or if you were to make a significant sum payment or a series of repeat significant sums, there is an opportunity for the banks to step in, question you about those payments and pause them. In our view, the banks should also offer us, as customers, the opportunity to tailor our accounts so that we can delay payments ourselves. That would mean that if we have been a victim of fraud previously, are at risk, or have received SMS messages inviting us to click on a link and feel that we might be at risk of fraud, we could contact our bank to say that we want to make sure that all payments over £25, for example—it could be a larger amount—are subject to a 48-hour delay. But banks are not configurable in that way.

The last thing I will say is around increased detection and prosecution rates. We know, as Simon Fell just said, that law enforcement is not resourced to deal with the scale of the problem. There is a Crown court case going on just down the road from here today—a significant fraud case that has affected more than 4,500 people. That investigation and prosecution has taken five years to get to court. The hearing was delayed—it should have started earlier this year—and it is looking likely that that trial is going to move on into next year. That particular case is caught up in some of the wider difficulties in the criminal justice system in terms of the speed of prosecutions and trials.

Louise Baxter: We could be more innovative in disruptions. We could disrupt the enablers. We could take the enablers out, which stops the criminals from working in the UK. There are ways to do it other than prosecution, on which we do not always share best practice. We are not great at being innovative in that space.

Q40 **Simon Fell:** I am going to come back to you on that; I just want to hear from John first.

John Kamoto: One of the biggest things we hear from other people is about changing the narrative. Louise mentioned the word "scam" earlier: people almost think you are not taking the crime seriously enough. I think we mentioned earlier that it is seen as a victimless crime.

Prevention is the biggest thing we can do to tackle the problem itself. With fraud, we cannot really prosecute our way, because 80% of fraud is cyber-enabled, and most of that is coming from abroad. In terms of prevention, there need to be regulations in place. Obviously, we have authorised push payment fraud, and the banks are doing a bit more now, but we think the social media companies, tech giants and so on need to do a bit more to prevent fraud in the first place. That is where we are going to win the fight.

The narrative change needs to happen as well, so that people can report fraud and we know the scale of the problem. I know we say that it is 40% of all crime in England and Wales, but it might be a bit more than that. First of all, we need narrative change, so we can get the scale of the problem, and then we need to work on the prevention side of things, which involves commercially and financially incentivising social media, because at the moment they are getting away with a lot.

Q41 **Simon Fell:** Back to you, Louise, on enablers.

Louise Baxter: The banks need to do more, in my opinion. As Wayne says, you sometimes get a phone call from the bank, saying, "Are you sure you want to make this payment?" Well, if they are phoning you, they know there is something untoward about it—there is the delayed payment.

In relation to disruption and enablers, I will give you a practical example. With white goods non-insurance policies, the direct debits are handled by financial management companies. We have met with all those companies—the ones that we think are involved. We said, "Do you know that you are dealing with these particular criminals?" They said, "No, we don't want to deal with them—that's fine." We said, "We will share information with you about the ones we know are criminals, and we want you to stop dealing with them," and they are like, "Fine." If they'd said, "No," then we would be looking at them for money laundering. They would be money laundering or aiding and abetting fraud.

It is similar to the work that we did with Royal Mail and the downstream access providers: the other mail providers, such as Whistl, Citipost and Secured Mail, that do not deliver to the door. We set up a system in relation to those to share information on the scam mail that was coming into the country. We were seeing that, if Louise at "Scams Ltd" had a contract with Royal Mail, Royal Mail would stop it, and I would just bounce it to Whistl. The criminals diversify from that, but it shuts it down, so they cannot get it in in bulk. You disrupt it, disrupt it and disrupt it—to the point that a criminal wrote to us, saying, "You've made it impossible for me to work in the UK." And I'm supposed to be offended by this?

We need to cut it off everywhere we can. If they are sending free pens, talk to the pen supplier. If they are sending free bits of cake, or information, shut down every bit that you possibly can around them to make it impossible. Hit them in the pocket. We do not have enough resources in my team to do the prosecutions over five years. That would take my whole team out, and we would not affect as many consumers as we do by doing the disruptions.

As law enforcement, we need to move on. The criminals move so quickly. They have far more resources than we have; it is like whack-a-mole. But if we can hit them quicker, with disruptive tactics, we are going to start to hurt them. We also need to work better internationally. We work quite well, but we are small. With that international sharing, the criminals do not target their own patches. You will get American or Canadian criminals targeting UK victims, because UK victims do not call the Canadian or

American law enforcement authorities—why would they? They will call the law enforcement authorities in the UK, if anyone.

We try to share information across the different law enforcement factions to ensure that they know what is coming from there so that they can take proper enforcement action. Sometimes they do not have any victims over there, so we do the victim impact statements for them. They can then take the civil redress case or the prosecution in America or wherever it is. That works quite well. Again, it is that disruptive piece—it is anything that we can do to stop it from gaining access to UK systems.

Q42 **Simon Fell:** Can I ask you about the information sharing you talked about—sharing lists of criminals who you know might be targeting individuals? I am interested in the barriers you face in doing that and the legal gateways you have to do it. Certainly, my experience in the past was that sharing information about susceptible individuals was really problematic, and we struggled with that under the legal frameworks we had. A lot of the banks, insurers and other companies were really reluctant to start to work together because of what they saw as structural barriers around information sharing. Do you feel that that has moved on?

Louise Baxter: I think that people hide behind data protection, if I am honest, and the Data Protection Act and GDPR. We are allowed to share information with law enforcement and if you do it for legitimate interests. If you have a room full of people who work in corporate governance or in relation to data sharing, everyone says something different, because it is subject to interpretation. We work very well with the Information Commissioner on our work with people being targeted on the telephone.

We do see some of those problems. Personally, I see it as an enabling Act, not as a barrier. While some corporate entities—banks, for example—might say data protection, a lot of that is competition as well, if I am honest, because they do not want to be exposed for having lots of scam victims. It has moved on slightly, but no further than when we spoke about it before, to be honest.

Q43 **Simon Fell:** Happy days. John, you were furiously nodding there.

John Kamoto: Yes. In terms of data sharing, I completely agree with Louise. They hide behind regulations—data protection etc. I know that at the moment stuff is going on in the background: Stop Scams UK is doing some stuff on data sharing. I am quite hopeful that something is happening at the moment, but more needs to be done in terms of leadership and the Home Office, let us say, to try to pave the way forward. Obviously the culture needs to change in terms of how banks try not to share that information, although the ICO says if there is a reason to share that data, you should. There needs to be a bit more leadership to actually try to get them to move forward.

Q44 **Simon Fell:** I will just ask one more question, if that is all right, Chair. You mentioned social media companies, so it would be remiss of me not to pick up on that. We know that, certainly for the banks, about 70% of the frauds they see carried across their platforms originate on social

media, which are clearly key enablers of all this activity. What should they be doing?

Louise Baxter: More. The Online Safety Bill probably does not go as far—a lot of the focus, rightly so, is on protecting children; I understand that. There is a lot of stuff in relation to tech companies and social media companies around things called dark patterns, which are nudge things. They mislead people and push them into making decisions that they might not have made had they not been nudged in that particular direction. It is almost degrees of crime, if you know what I mean. More needs to be done on these dark patterns and the work in relation to cookie fatigue; we are all just going "Yes". Most people think that if they tick "Reject" on cookies, they cannot access the website that they are trying to access. All it means is that their data will not be shared.

A lot of the stuff in relation to social media companies will start with an advert that is a data-mining situation. Again, that is the start of your suckers list. More needs to be done at that early stage. We find with scam victims that early intervention is key—get in early, and you are more likely to effect a change and not then have to undo coercive control or grooming, instead dealing with it as a trauma response. If you get in much earlier on in the journey, you are likely to prevent that person becoming a repeat victim.

Social media companies could be proactive as well in their education campaigns. They have platforms where people will listen. They could be far more proactive than reactive. A lot more needs to be done. They could take down websites a lot quicker than they do.

Wayne Stevens: Victim Support was one of the organisations that campaigned to bring in the responsibility on social media platforms to police paid-for advertising, so we were really pleased that the Government included that in the final Act. People are defrauded through social media accounts, and we have seen a lot of that in the past couple of years.

I have an example here: someone called Lizzie we worked with. She received a WhatsApp request from someone purporting to be a friend, but it transpired that it was someone who had been able to hack into her friend's account, which opened up hundreds of contacts with people to whom the fraudster could then represent themselves as a friend.

We believe that social media companies also have a responsibility to try to prevent bad actors coming on to the system through proper verification when someone signs up for an account. Some verification steps are needed to demonstrate that someone is a proper person, whether that is by country of residence or by reference to another key piece of identifying information, but they should be who they say they are. As Louise said, social media companies have a very powerful presence in being able to speak to their users—"An impersonation fraud is going on at the moment. You might receive a text telling you that this is your daughter and she has lost her phone"—but they did not do that.

Q45 **Simon Fell:** Out of interest, would you support a "polluter pays" principle for social media?

John Kamoto: Yes, definitely. I think that is the single most transformational policy you could do. As you said, energy companies have the carbon tax, and when 80% of all fraud is being enabled by tech giants and social media companies, it is almost stupid not to have one. I think, definitely, they need to be in some kind of paying mechanism, as has been done with the banks with authorised push payment. If there were some kind of reimbursement model, we would definitely champion that as well.

Q46 **Simon Fell:** Wayne, you are nodding along. I assume you agree.

Wayne Stevens: Absolutely. Bearing in mind that the Online Safety Act will be regulated by Ofcom, there is the question of how well resourced Ofcom will be. How much of a priority will it be for Ofcom to investigate and enforce?

Louise Baxter: I liken this to some of the work that has been done in gambling. There is a levy now that will hopefully be placed on the gambling companies. I know that they are legitimate companies, but it is for supporting people who have suffered from gambling harm.

This can be looked at from a banking perspective or a tech perspective—if they are involved in that and making money from it, potentially there could be a levy or something that is pushed to support or to provide a better, more enhanced and fit-for-purpose victim support service, which we lack. There's different ways to look at it, isn't there?

Q47 **Alison Thewliss:** First, I will ask about the types of fraud that happen on platforms. Figures from TSB, for January to March last year, state that 70% of the frauds that it was picking up were being perpetrated on Meta—24% on Facebook and 46% on Instagram—4% on Snapchat and 23% across other platforms. I wondered if the types of fraud varied by platform. Perhaps younger people are being targeted in a particular way, on Snapchat, or older people on Facebook. Will you talk a wee bit more about that?

Louise Baxter: Facebook is a different demographic from Snapchat, TikTok and things like that—she says. But my daughter is 13, so I have Snapchat so I can spy on her. A lot of the time, some of the scams you see on Facebook are impersonation scams. Martin Lewis spoke out recently, didn't he? His face was being used on adverts that were not legitimate.

Also, there is quite a lot of data mining—"Enter this free draw to win prizes" and things like that. Again, they are data-mining scams. You will see quite a lot in relation to TikTok Shop and Snapchat, and Instagram is quite prolific in relation to money mules as well. This involves targeting younger people. It's like an employment scam. Basically, you become a money mule: criminals put money into your bank account; you bounce it on and you get to keep a little bit of it. But you become part of the criminal organisation; it's a way for them to hide it and money launder.

As Wayne said, you see impersonation scams in relation to WhatsApp. And you now see text message scams, where people are sent a message saying, "Mum, I've lost my phone," and then they push you to different platforms. Money muling is a problem for younger platforms, where they can put up adverts. Then you have the data-mining ones that are surveys. Again, they collect so much information about you from a simple survey. Or there is the one where they say, "Let's find out what your personality type is," and then you put in all your personal information, because you don't realise what you're doing—it will be things like your kids' names or your pets' names, which are people's passwords as well—to get a funny selection at the end about what sort of personality you are.

So it's all different types, all the time. We still see home-working scams as well. And doorstep crime is still prevalent for older people. We still see a lot of doorstep crime—door-knocking. Especially with the storms, we have seen a lot of that as well. In relation to some of the other social media platforms, we have seen old-school rogue traders, who would door-knock, move on to those online platforms and advertise on there.

So if somebody puts up a post that says, for example, "Does anybody know a good roofer?" or "Does anybody know a good gardener?," the criminals will say, "Yes, I'm a great gardener. I do it for this." You are seeing a lot of that. In relation to websites that consumers might think are trusted, criminals are moving on to those websites, because the checks are not being made on those particular websites.

Q48 **Alison Thewliss:** As a consumer, if you are on one of those local Facebook groups or something of that kind, what can you do to interrogate those kinds of things? Would you just say to people, "Avoid it altogether. Don't take any recommendations there"? Or how would you advise them?

Louise Baxter: From the perspective of getting a trader, the advice would be: use a reputable good trader scheme, like TrustMark, Buy With Confidence or Which? Trusted Traders. They would be the three places where we would push people. We also advise people to take recommendations from friends. Your friends are on Facebook. So you have to do pre-checks.

It's around this education piece; make sure that you do pre-checks. I met a lady the other day. She still had building work going on; it had cost her £60,000 and it hadn't been finished. She had found the builder on Facebook. They had not done the work properly. She had had to pay for someone to come and fix it. They had run out of money. She still hadn't got it fixed. Her partner—it caused so much stress for them, and they had disabilities. It was an incredible amount of turmoil for the, I think, three years it had been going on. She took this recommendation at face value. She said, "If I had just googled them, I would have found out. I would have seen all the negative information. But I didn't, because I took it on trust."

I am generalising, but sometimes people of a certain age are more trusting with people at the door. We used to have this with, for example, scam mail: "Well, it's delivered by the postman!" They trust the postman; they see the postman every day. So it's a case of trying to break this way we think about things and get people to be a bit more cynical—which is sad, isn't it?

Alison Thewliss: Scepticism is quite healthy with these things.

Wayne Stevens: Louise has given a fairly comprehensive list of the sorts of frauds that you might come across on social media. I would probably add pension and investment frauds, whether that is paid-for advertising, which will become illegal of course, or cryptocurrency promotional schemes, which may involve paid-for advertising but may be much more likely to be promoted among much more informal networks.

John Kamoto: I was actually talking to TSB yesterday and asking them what kinds of fraud they see. I think there has been mention that around 87% of all investment frauds come from Meta; that is a scary number when you think about it. And I think 20% came from Google. So you can see how much these sites are fuelling the flame, as it were.

Q49 **Alison Thewliss:** I remember vividly hearing somebody who was targeted for investment fraud not just once but twice. It's kind of difficult to understand how somebody, having been rinsed at one point, will then go back to that. Do you have any thoughts—aside from the sucker list point that Louise set out—about why people end up being targeted in this way and susceptible in this way? And can more be done to safeguard folk when they have been defrauded once?

Wayne Stevens: In terms of pension and investment fraud, we worked with someone who lost a significant amount of money over quite a short period of time. It transpired that the person purporting to be from the investment company effectively groomed this person over a period of time. There was an investment opportunity, he was sent some screenshots of a piece of software that looked like it was generating returns, and he was drawn in over quite a lengthy period of time. When someone in his family said, "Dad, you're being defrauded. You've got to stop doing this", he cut off his contact with the fraudsters. He was then approached by companies saying, "We're sorry to hear you've been a victim of fraud. We can help you get your money back." So, he thought, "Oh good. That's a good thing." It will, no doubt, have been linked to the original organised crime gang, but he was subsequently defrauded on a couple of further occasions, with companies saying, "An upfront payment. We'll do our first bit of work for you and come back with some intel, and then you can pay us according to how complex this investigation and recovery might be, bearing in mind it will be international." It is so plausible.

Alison Thewliss: They want to believe it is true.

Wayne Stevens: Absolutely plausible.

Louise Baxter: You find with people that it is a rationalisation trap a lot of the time as well. Also, the shame around it makes you think that they do not want to talk to their family members, so they are trying to recoup it and get it back. Therefore, because they are not sharing or talking, they are stuck in this hot state in relation to it—it is really difficult.

I think about 11% of people become repeat victims. I have seen victims who I have been to visit again and again, I have got adult social care involved, and I have talked to them and talked to them, but they will not stop responding. It has become such a part of their daily life and daily routine—and their purpose as well. Some of the time you will see, not with all older people but some older people, that it becomes part of their purpose and their contact as well. It is very difficult to go, "Your 'friend' is stealing your money." That person has become their friend or their contact. You see it with doorstep criminals as well who visit. They bring cakes and flowers, they come and chat, and they have a cup of tea. There is a whole element of that relationship side of things.

With romance scamming, and specifically pig butchering, that starts sometimes with the romantic interest over a social media platform where somebody will form a relationship with you. They will become your friend or a potential romantic interest, and then they will go, "I've got this great investment opportunity for you", which will be crypto-based or something like this. Again, the people committing the crime are being people trafficked, so they are part of the criminal organisation, and it is all linked to human trafficking as well—they are being abused and forced to commit the crimes as well. You end up with people going, "They're my boyfriend", "They're my girlfriend", or, "They're my best friend. I've been talking to them for six months—of course I'm going to invest in this amazing opportunity that they've given me." Then they invest, they receive a little bit of a return—as you say—and they say, "It can't be a scam because I've had a bit of money back." Then it is, "Okay, your investment is really high now. Do you want to take it out? It's £4,000 in fees." Then you never hear from them again. Those people will be left not only without the money but in a situation where they have lost their "friend". They have lost the person that they are talking to. We do not deal with all of those other things when we are trying to support a victim of scams or fraud.

Q50 **Alison Thewliss:** I have a lot of students in my constituency and lots of universities. Can you tell us a wee bit more about the risk around money muling, what happens to young people, and how they are drawn into that?

Louise Baxter: That generally starts with adverts on social media platforms going, "Do you want to earn a quick £500?" They will then use that student's bank account. The criminals will bounce the money to avoid any suspicious activity on their own bank accounts or opening new bank accounts. I am too old to be a student, but let's say I am and they use my bank account. They bounce the money in, they leave me £250, and they move it on—so they bounce it really quickly. What can end up happening is that I then become considered to be a criminal and my relationship with my bank can be exited. My credit rating is affected. I could be

prosecuted—again, because I am part of the criminal organisation if I am knowingly doing it as well. It can affect my credit. It can affect my facility to get bank accounts in the future. It can have quite a huge knock-on effect. We also don't do budgeting and financial education, but we should do that because it would help and assist with this.

On teaching young people about things like this, how do you make it land with young people? Think about counterfeit goods, which are fraud, as well. People want to buy counterfeit goods because they are cheap, and people don't have a lot of money at the moment. How do we make them care about fraud and counterfeit goods? You make young people care because their grandparents could be scammed, and young people care about their grandparents. You teach young people anti-fraud messages and say, "This could be your nan. Don't let your nan get scammed." Then, when they come out of school and their grandparents pick them up—a lot of parents are working now—the children tell grandparents, and the grandparents listen to their grandchildren. They don't listen to their children—my mum does not listen to me, but she listens to my children. Then you get that vicarious education all the time. There are loads of studies around peer to peer but also grandchildren to grandparents to get those messages out there as well.

Q51 **Alison Thewliss:** I am conscious of time, so I want to ask quickly: is there more that universities could do to let students know about the risk they are putting themselves under?

Louise Baxter: Yes, there is education they could do. Again, using social media in a positive way, there could be some really proactive social media campaigns for students specifically, trying to make it relatable. That is something we could talk about doing.

Q52 **Tim Loughton:** We have heard about lots of different sorts of fraud. What is the most prolific and fastest-growing form of fraud, in your experience?

John Kamoto: It's a hard question to answer because there are so many of them. The fast-growing one that we have been working on is authorised push payment fraud, which has been rising. This is obviously because of the move to online banking and the faster payments system, among other things. That is the one that is causing the most trouble because it happens almost straightaway—you send money to the fraudster, and they have run away with the money already. That is what is causing the most problems at the moment because it happens so fast. When it comes to which kind of scam the fraudster uses to do that, there is all sorts, really.

Wayne Stevens: I was looking at the UK Finance figures; they did a report that came out in September. The biggest fraud by volume is around purchase fraud—people buying stuff over the internet predominantly. That is the single largest—

Q53 **Tim Loughton:** Largest by what? They have the details of your credit card and they are just impersonating you like that.

Wayne Stevens: Yes, they are impersonating legitimate companies or sellers selling goods, products and services.

Tim Loughton: So the sellers, not the customers. They are selling stuff which they—

Wayne Stevens: Predominantly selling stuff. But there are also people posing as sellers who are getting people to send goods out so that you think that you have bought something, and it never turns up.

Q54 **Tim Loughton:** But that has to be on a platform.

John Kamoto: Yes. It could be Facebook Marketplace, for example. Say someone is selling a product there and they tell you, "These are my contact details and my bank account. Send me the money now", and you do that. Again, they will run away with the money because of the payment system that is being used, which is authorised push payment.

Q55 **Tim Loughton:** Okay, so the accomplice after that fraud is the host site, surely.

John Kamoto: Yes, it is facilitating the fraudster, in a sense.

Q56 **Tim Loughton:** So there is a straight line of responsibility. What is that company then doing, first to retrieve the money from the person who has used their site, secondly to make sure they are not able to use it again, and thirdly to report it as a crime?

John Kamoto: At the moment, I would not say there is not much going on. Obviously, in the background, there is the voluntary fraud charter, which we will hopefully see next month or at the start of next year. As Wayne has already mentioned, there was a missed opportunity with the Online Safety Act in terms of what more these companies could do—I don't know if a voluntary charter is going to have that many teeth. We had the same with the banks, with the CRM code, and two years later we had to go to regulation to mandate them to do something about it. I am afraid that might happen again. As I keep saying, the platforms need to do something to prevent fraud from happening in the first place if we are going to go anywhere here.

Q57 **Tim Loughton:** That is where a lot of this seems to be coming back to—whether it is the romance fraud we were talking about earlier, which is done on Tinder or an equivalent site, or whether it is one of the platforms offering a marketplace or whatever. If they did not exist, that fraud could not happen online. This has proliferated because of the use of social media and the internet and the way we transfer our money these days.

John Kamoto: Yes, definitely.

Q58 **Tim Loughton:** In the old days, you went along to a shop and you bought something. If they did not deliver it, you went back to the shop—you knew where the shop was. Now, everybody is online. They can disappear and make up a character online. I think what you are saying is that the internet platforms have a far greater responsibility to prevent,

retrieve and report.

John Kamoto: Yes. Like I said, I am slightly hopeful, because I heard that the Security Minister was in the States and talking to the companies recently, so we are seeing movements there. But since the consultations we had in the summer, we have not really heard much, so we are just waiting with bated breath to see what comes out of it.

Q59 **Tim Loughton:** I never used to do any internet banking, but it has become the case that you have to do internet banking. Actually, I quite like it; it is so easy and so effective. If I purchase something online, I have to go through a series of, "What sort of transaction is this?" and "Are you sure?", and I have to tick a box to say I have been made aware of that. It might then ask me to do my iris recognition to make sure it is actually me doing it, rather than somebody else. So, there are a series of measures.

If I am buying something with a credit card, there have been a couple of cases in the last few years when I have had a telephone call to say, "We think there's been irregular activity." For me, it always seems to be somebody buying dresses from a cheap dress shop, which is not what I tend to do, and they prevent it. My experience has been that my bank or credit card companies have been quite good. Am I an exception? Does that service not apply to everybody? Do they need to completely up their game? What could those companies be doing that they are at present choosing not to do?

Wayne Stevens: What we see with the very frauds that you have described is that people get persuaded not to use the embedded payment system within the platform. They will say to you, "Oh, don't use PayPal; it takes a cut," so you will be asked to make a direct bank transfer. That is a very, very common feature.

Louise Baxter: Now, the criminals are trying to avoid the bank's authorised push payment system by sending you a bank card. It is like a GoHenry card, but it is not GoHenry—the ones for children.

Q60 **Tim Loughton:** What's GoHenry?

Louise Baxter: GoHenry is for children. If you want to give your kids money, they can have a debit card, but they will only have what you have put on that particular card. It is like a gift card. They are sending consumers those, so consumers are transferring money to themselves. The criminals set up that card in their name. That card will be for Louise Baxter, so when I go on to my bank, I will be transferring money to Louise Baxter. On that card, I will then transfer to the criminal. I had this with a chap that I spoke to this week. What happens is you cannot get your money back because you have not transferred it to a criminal, so the banks then have no responsibility to pay you back. The criminals are less likely to be detected from that perspective, because they understand that if the banks will have to refund unauthorised push payments from me to them, their accounts are going to be shut down by the banks—it is going to be beneficial to the banks to shut them down.

In March 2020, we went from bricks to clicks, with no training on how to do that safely. Obviously, we were dealing with quite a lot of other stuff at that particular moment in time but think about people over 75 who used to go the shops. They were told that they had to buy everything online, without any education on how to do that safely. What you will see is that it not just the platforms; websites spring up all over the place. They spring up quickly, and then they go away. We saw it at the beginning of the pandemic, when they sprung up selling masks and hand sanitisers at £50 a pop. What they do is they sell you that and you never get it, so there is your first scam. Your data is then sold on and you are retargeted and retargeted. The social isolation grows because we are not able to contact those people—how do you educate people who are socially isolated? It is really difficult to do that. The websites spring up and bounce off. The internet is like the wild west. There is a responsibility on consumers to do some checks, but, again, it is easier for the tech companies to take the sites down than it is for us to keep on top of how many sites are out there.

Q61 **Tim Loughton:** What single, simple thing could an ordinary punter do to ensure they are safe? It seems there is no Green Cross Code equivalent for when you are dealing online. You came from East Sussex. I remember a few years ago the Sussex police and crime commissioner produced a scams guide specifically for older people, which was quite widely distributed—it was a good thing. I wonder how many people actually got it and then read it. Should there be some campaign that has those simple messages to make you think twice and that sets out a series of checks that anybody could do for the basic stuff? Obviously, it gets more sophisticated. Who is responsible for that?

Louise Baxter: That is what is coming at the moment from a Home Office perspective. There is one campaign that hopefully everybody will jump on board with, and that uses one message. There are so many anti-fraud messages from different organisations, and none of them land because everyone goes, "Well, that's not going to happen to me. Actually, I'm really busy, so it's not relevant." We need one message and it needs to be simple. Even with things like the internet, there is a really simple thing called Get Safe Online, which is a checker website. You just put the website in, and it tells you whether the website you are trying to buy from is safe. It pings you back straightaway. It gives you a RAG rating—green, red or orange—and then you make a decision based on that.

Q62 **Chair:** What is that called again?

Louise Baxter: It is called "Check a website" on the Get Safe Online website. It is really easy to use that piece of information for people who are internet-savvy.

Q63 **Tim Loughton:** Who runs that? I have never heard of that.

Louise Baxter: Get Safe Online. It is through Cifas, which is an organisation that educates people on shopping safely online and how to maintain your internet safety.

Tim Loughton: Never heard of them.

Chair: No, never heard of them.

Louise Baxter: It is a really easy tool to use. We need to verbally share those messages with our neighbours, our mums, our dads, our aunties. We need to talk about this. That is the only way we are going to get those messages to land. It is not taking away people's autonomy and doing it for them, but if they are doing it, it is supporting them to do it. Again, we still blame and shame a lot. People are not going to ask for help or support if we are making them feel stupid or ashamed for not knowing something. It is situational vulnerability or marketplace vulnerability. With all the green energy stuff coming down the track, we are entering into a storm at the moment. It is going to get worse.

Q64 **Chair:** In terms of the Government's recent fraud strategy, there was going to be a victims of fraud working group set up, and I think you are all listed as members of that. Has that group actually met?

Wayne Stevens: Yes.

Q65 **Chair:** It has? Okay. Was that recently? Was it just one meeting?

John Kamoto: There have been a few meetings. It started in the summer. One of the first meetings was mapping out the victims' support environment; we are still waiting on what we are going to do with that. There have been a few meetings, but at the moment, it is more mapping out what each organisation does to see if we can work together closely going forward.

Q66 **Chair:** So no actual actions yet from that.

Wayne Stevens: Not yet. We have been waiting for the fraud strategy for quite a long time because it has been delayed. It is a very useful information exchange and partnership update group. There are some dedicated Home Office staff who have been servicing it, and there are some key players round the table, such as the Serious Fraud Office and the City of London Police, as well as the Home Office. It would be good if it had a role in helping to deliver the fraud strategy—the third pillar around empowering the public and providing services for victims—but in order to do that, I think it will need resourcing.

Q67 **Chair:** Generally, what do you think of the fraud strategy? Do you think it will help victims?

Louise Baxter: Doesn't go far enough.

John Kamoto: It doesn't go far enough at all. Also, with the target of 10% by the end of this Parliament, it is not really forward thinking, is it? It is just thinking until the next election, which is not great. This problem is so big that it needs a lot of forward thinking.

Louise Baxter: And some of it hasn't happened yet, so we cannot see what the outcomes are.

Q68 **Chair:** What progress has been made on the national roll-out of the multi-agency approach to fraud in England and Wales?

Louise Baxter: Currently 28 of the force areas are active in the multi-agency partnership work. There was a pilot run, which was originally funded by the Home Office for this, but is not funded by the Home Office any more. We resource it within our DBT budget. We have two force areas that are not engaged; the rest of the force areas are engaged. There are varying degrees of how much engagement there is, but we feel this is one of the best ways to help people from a resource perspective and from a supporting best practice for victims perspective.

Q69 **Chair:** Which two are not engaged?

Louise Baxter: I can tell you—I have them written down, but it is over there in my bag. There are two that are not engaged and there are resource issues.

Q70 **Chair:** I am going to bring Simon in to ask the final question. Do you think that Action Fraud's replacement will work with victims and support victims better? What does it have to do?

Wayne Stevens: You'll obviously be aware of the HMIC inspection reports from 2018 to 2021. Action Fraud's service has not served victims well in recent years. We don't know yet what the new service will look like. It will need to collect reports from victims and will need to be accessible. Victims will need to trust it and it will need to be able to pick up the data that helps the investigation and detection of crime. That is the primary purpose of this single national reporting tool. We welcome that. Organisations like ours will need to drive people towards that if they have experienced fraud or if fraud has been attempted.

However, it is not a support service. The effectiveness of Action Fraud in not just capturing data but also helping victims, providing information and patching them into local services such as Age UK or us or trading standards will be key to its success.

Q71 **Chair:** So we are still waiting—

Wayne Stevens: We are waiting to see what that might look like.

John Kamoto: From what I have heard, it is mainly going to be an online reporting tool. With older people being digitally excluded, we are not happy about that, so we are hoping there will be people manning the phones. We are still waiting to hear.

Louise Baxter: With people being expected to do online forms all the time, the room that we are in now is not reflective of the true population. With the average reading age of people being 12, they do not understand the information that we are trying to get to them. People generally don't go, "I don't understand that," because they do not want to be made to feel stupid. We have to provide, like you said, the telephone service, the internet service, the online service. Again, I am generalising, but people with anxiety disorders do not like to speak on the phone, so they need to be able to email or put it in writing. We have to ensure that we design all of our services as best we can with inclusivity in mind, to ensure that we

capture all of that vulnerability. We are not particularly good at doing that yet.

Chair: No.

Q72 **Simon Fell:** We are running over, so I will be brief. This has come up a few times—in the first panel and in this one, too. We are not just talking about a financial crime. On the first panel we heard about coercive control and the hideous impacts of that. We know from money muling that people may not have access to a bank account if they engage in that. There is social isolation and all kinds of things like that. We all have examples from our constituencies of people who have been badly affected by this crime, but it is not necessarily quantifiable in pounds and pence. I am interested in your final thoughts on whether we do a good enough job of capturing what the harm of this crime is. If we are not, is that what is driving the poor response and the lack of support from the Government and Treasury to get a decent response in place?

Louise Baxter: I do not think we know the true costs of the harm in relation to this. From a wellbeing perspective, we know that when we have fitted call blockers in consumers' houses, we have assessed their wellbeing status and it has gone up by two to three points once we have put in a call blocker. That is a societal saving of about £2,000, because they will potentially need less access to public services or adult social care from the wellbeing perspective, and they will engage more.

On the knock-on effects, you are 2.4 times more likely to go into residential care or die within 12 months of being scammed in your own house. The knock-on effects are catastrophic from a wellbeing perspective. I do not know whether we can put a monetary amount on that, but the harm is incredible. As Wayne said at the beginning, it could be £5 or £5 million—it is not the financial amount that matters; it is the harm it causes to that particular consumer, the mental health effects—all of those things—and whether those people can access the support they need afterwards. We do not provide bespoke victim support. Again, we paint it all with one brush—fraud is fraud—but victims of romance scams, investment fraud and lottery scams need different support. One shoe does not fit all; we need different bespoke victim support for those people.

Wayne Stevens: The figures around fraud suggest that it is massively under-reported. It may be that as few as one in seven frauds are reported. For us, the key first step is encouraging and supporting people to report fraud, whoever they are. Many people think, "Oh, it is a civil dispute," or, "I've been foolish." People do not necessarily see it in technical or legal terms. If that information does not get into the national reporting service, then we have only a very small part of the picture: we do not understand the true nature of the fraud, who the fraudsters are, where the fraudsters are, or how to help the people who are most impacted by it.

John Kamoto: I completely agree with that. It is about fostering an environment where we are able to talk about it—that is when we find out

the true scale of the problem. Then we can try and tackle it. But at the moment, I don't think we can put a number on it.

Simon Fell: That is really helpful. Thank you very much.

Chair: That concludes the second panel. Thank you very much indeed for your evidence this morning; it has been very enlightening. I have to say, I am going to stop clicking on the "Accept cookies" button—from what you have just told the Committee, I am going to at least do that.

We will carry on with further sessions on this inquiry. You have given us lots of things to think about and questions to ask—thank you for that.

I should also say that we have a survey that we will advertise on social media to try and get further information from victims of fraud to feed into our inquiry to ensure that we understand as best we can the range and the effect on victims. If people feel able to fill in that form, that would be very helpful to the Committee and our inquiry deliberations.

Louise Baxter: Be careful with that—we are saying not to give your information on social media via surveys, and then we are doing a survey saying, "Can we have your information as victims?"

Chair: We need to speak to you about making sure that our survey does not do that.

Wayne Stevens: We are also saying not to click on links or unexpected pop-ups.

Louise Baxter: We just need to be a little bit—

Chair: Can we call on you for some assistance to make sure we are not doing anything we shouldn't? We want to keep all that information very safe.

Louise Baxter: Yes, absolutely.

Chair: Thank you very much.