Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 3 March 2022

9.30 am

Watch the meeting

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

Evidence Session No. 2 Virtual Proceeding Questions 13 - 22

Examination of Witnesses

Arun Chauhan, Katy Worobec and Mike Haley.

Q13 **The Chair:** Welcome to this evidence session of the Fraud Act 2006 and Digital Fraud Committee. A transcript of the meeting will be taken and published on the committee's website, and you will have the opportunity to make corrections to that transcript where necessary. Many thanks to our first panel this morning. We are joined by Mike Haley, who is the CEO of Cifas; Arun Chauhan, who is the trustee director of the Fraud Advisory Panel; and Katy Worobec, who is the managing director of economic crime at UK Finance.

We have lots to get through and lots of questions for all three of you. In the interests of time, we will try to direct the questions to particular panel members. If others would like to come in, please indicate, and of course I will bring you in.

Q14 **Lord Vaux of Harrowden:** Thank you and good morning. My question is a general scene-setting question for Katy Worobec, if that is okay. Would you be able to describe the most common business models used by fraudsters today and perhaps explain the term "kill chain" in that regard? It would also be interesting to know whether any common themes arise from those various types of business model. Would concentrating on any particular one have, as it were, a disproportionate, positive impact on it? If you had any views on the extent to which fraud is a domestic or

international problem, that would be helpful. Do you expect to see any trends or changes in the future?

Katy Worobec: There are quite a number of questions there, but I will attempt to remember to answer all of them if I can. Good morning, everybody, and thank you for inviting me to give evidence today. The most common business model from the frauds we are seeing in the industry is that of targeting the individual as the weakest link in the chain. Over the years, and I have been working in the industry for a number of years, the industry has put a lot of preventive measures in place to tackle things such as card fraud and unauthorised frauds, but we are seeing that the fraudsters have circumvented that and are targeting the individual. They do that, as I am sure you are aware, through social engineering, often on online platforms or by phone, to get the personal information in the first place, and then use that information to dupe the customer into making payments from their account into another account.

That is the basic premise. We are seeing an increase in fraud, and that is likely to continue because it is quite difficult to detect when that has happened. This comes into the kill chain question that you asked. If you think about the way in which the fraudsters work, they are doing the social engineering up front and getting the information perhaps by getting the victim to put their data on to a fake website. They then reuse that information to give credibility when they next contact the victim and pretend to be from the police or the bank. They direct the victim to make the payment, and it is only at that point that it hits the banking system. There is a limited opportunity to detect and prevent that type of fraud.

Similarly, at the other end, when the victim makes the payment to the receiving bank account, there is a possibility of spotting where that bank account is receiving funds, but it is quickly moved out and then cashed out, often into cryptocurrency for example. Again, there is a limited opportunity to do much from the banking industry's perspective. It is certain that the fraudsters are very adept at spotting the weakest link in any chain and exploiting it to the best of their ability.

The themes that come out of that certainly build on world events. In the current Ukraine crisis, we are already seeing people setting themselves up for fake donations to Ukraine, for example. In the Covid crisis, they were setting themselves up to sell fake equipment or other things that were top of mind among those who were experiencing problems during the pandemic. They use world events all the time to add credibility to the way in which they operate.

That is the key background. This type of fraud, in which the victim is targeted, is likely to continue to be an issue. This is why it is particularly important not just for the banking industry to tackle the problem, but for online platforms, the telecoms industry, regulators, government and law enforcement all to come together and try to tackle this thing from cradle to grave.

Lord Vaux of Harrowden: Did you have any views on the international

aspect?

Katy Worobec: Thank you for reminding me. I knew I would forget at least one of the questions. On the domestic front, it is often quite a challenge to tell where these fraudsters are operating from. It can be quite challenging to know, simply because they tend to use online platforms, and it is not necessarily easy to determine immediately where they are operating from. We know that the UK tends to be a target for fraudsters. As much as anything, it is to do with the fact that the English language is often used as a world second language, as we know. It is true that we are seeing a number of fraudsters operating from outside the UK, so it is extremely important to ensure that we can forge links with other jurisdictions to get information and tackle fraudsters who are outside the UK.

Mike Haley: This is not to say that authorised push payment fraud and scams are not a significant and growing problem, but the most significant number by volume of the cases filed to the national fraud database across 13 sectors is identity fraud. We have 360,000 cases filed by our members that cover the banks, the credit industry, the telecoms industry and retail. Of those 360,000 cases, 63% were identity fraud.

The business model there is slightly different to that of scams, although it uses a number of the same techniques. The business model there is really about harvesting personal information. That can be from data breaches, and our personal information is traded on the dark web and dark web sites, which are criminal sites for exchanging information. There is an awful lot of impersonation of banks, figures or authorities such as the police to get personal information.

Probably all of us have received an unsolicited email or text message with a malicious link, usually asking for personal information and credentials. That information is taken from different sources, and the criminal enterprise then either impersonates a genuine person or creates what we call a synthetic identity to make applications for bank accounts, credit cards, loans or mobile phones at scale. Literally tens of thousands of applications are made in the online environment, and 91% of those identity frauds are through the internet or mobile devices.

That has all the fingerprints of organised crime because it is at scale. It is over the internet. It is an impersonation not of a single individual but of many individuals. It is very difficult to tell the balance between domestic and international, because when you have an attack through the online world, it is hard to track whether that internet-enabled device has been bounced through a number of jurisdictions and providers. I believe there is an amount that is international, but there is clearly domestic organised crime targeting UK citizens and institutions as well.

There is a different business model. There is some specialisation in the different steps, so if someone is very good at creating the malware, the link creates what looks like a really good impersonation, say of a bank, and you get an email that looks like it comes from your bank. They send

that to millions of people knowing that, of those millions of people, a certain percentage will have an HSBC account, for example. Someone creates and sells the malware, someone else will harvest the personal information, someone else will make the attack, and someone else will take the money and route it through their mule accounts. This is a quite sophisticated, but loosely organised, crime network. It is not like a mafia network where they sit around the same table; they all have credibility from the forums that they engage in for their very specific roles.

There are different models of sophistication depending on the fraud type. We know, for example, that quite a lot of romance fraud comes from overseas. We even know that there is a specialisation in romance fraud in certain areas of West Africa. We know that as there has been some law enforcement activity working with the Ghanaian and Nigerian authorities.

It is very difficult to put our finger on where identity fraud is coming from. There, we need some of the resources that we use in national security—for example, the National Cyber Security Centre—to help identify where this is coming from and who is behind it. It is quite a sophisticated enemy. When we deal with it on a domestic basis as individual institutions, we have one arm tied behind our back.

Arun Chauhan: I just have two points on the business model. If I could characterise one business model as this, it is impersonation from a distance. Mike has quite correctly identified that this is an international operation. There is organised crime, but it is often impersonation from a distance using online platforms or other means to convince an individual that they are dealing with a legitimate enterprise. There is a real issue of proximity from the perpetrator to the victim, which is why it is such a hard crime to follow through with on prosecution.

Mike is quite right about the trading of data. We need to be alert to how easy it is to talk about trading data on social media sites, almost. There is a site called Telegram, for example, which is a bit like WhatsApp. People will trade "fullz". Fullz are someone's full details. "Do you want to have Arun's fullz? You can. Just send me £50 and I'll send it across". That type of platform is operating in the UK, but it is based overseas, nobody really knows where. Those are the types of issues with the business models that we are trying to combat.

Q15 **Viscount Colville of Culross:** Good morning. I would like to start by directing my question to Mike. You have said that fraud is perceived by those in authority as less important than other crimes, and the police have been criticised by HM Inspectorate of Constabulary for treating it as a low priority that does not cause harm. Does this perception colour the way the police deal with individual frauds, particularly digital frauds? You mentioned romance frauds, but there is also money muling. You told us earlier that 51,000 accounts in the UK alone were held by money mules. Is this perception a problem? Does that create a problem for trying to tackle these sorts of frauds?

Mike Haley: Yes, it absolutely does. For too long, fraud has been seen as a victimless crime that somebody else picks up the tab for—it might be a big institution like a bank—with no real impact on individuals. In fact, it is very well documented and researched that fraud, beyond the financial impact on an individual, can be as impactful as any other crime. I could be burgled and everyone would have sympathy for me. I would not feel shame or embarrassment about it, and other people would have some empathy. With a fraud, there is a degree to which people will feel ashamed and embarrassed to even speak about it. They feel, as do others, that they have brought it on themselves in some way, they were not very savvy and they were taken in by social engineering.

There is more generic thinking around fraud being victimless that seeps into policing. There are also issues of where the fraudster is and the policing model, which is set up on the basis of managing the criminals and the crime in the locality, whereas fraud victims can be anywhere in the country. They are usually dispersed, so there is an issue with accountability. Who should be responsible for investigating fraud? If I go to my local police say in Warwickshire and they say, "This looks like it's come from somewhere in Newcastle", it is passed from pillar to post. If you are in Newcastle and no one has been affected locally, it does not become a political issue for the chief constable or the police and crime commissioner.

We are trying to deal with a national issue where victims are dispersed and a model of policing that was set up to deal with very localised crime, as is also true with trading standards for example. Trading standards deals with quite a lot of scams, but it was set up for local markets. Trading standards has a long history, but we now work in international markets. The internet and digital routes mean that that is the case for everyone.

I agree that it colours everyone's view of how important fraud is. It is not a crime that people speak to others about because there is this embarrassment and shame about being a victim of fraud. Therefore, it is underreported. We need the bravery to make it a priority. It is now 40% of all crime. Fraud Crime is very impactful and affects people psychologically. They lose trust in friends, families and institutions. People do not go on the internet again. This has all sorts of effects. That embarrassment and shame is something that people carry with them. It is very harmful. We have seen plenty of vulnerable people who do not engage with others afterwards, so there is an issue of loneliness then. They cannot share this as a problem.

Viscount Colville of Culross: I understand the embarrassment of the victims, but do you think the police are not taking it seriously enough not just because it is underreported but because they just do not think it is an important enough crime?

Mike Haley: Yes, I do. Certain parts of the police, such as the City of London Police, which is the lead force for fraud, take it seriously. Generally in constabularies it is not part of the policing requirement or

the priorities of policing. Therefore, a chief constable will not make it a priority locally. They are also ill equipped, so they do not know where to start. You do not want to start fraud cases if you are not going to clear them up and your statistics are very poor. There are all sorts of factors, but policing does not see this as a priority and has not for a long time. I think that 2% of policing activity is put into fraud, when it is 50% of crime. I think we saw 6,500 fraud prosecutions out of 500,000 prosecutions last year by the CPS. It is not taken seriously throughout the whole system.

Viscount Colville of Culross: We are talking to Lord Agnew after this session. He has also said that there is a problem in government with dealing with this issue and that the Treasury has little interest in the consequences of fraud to the economy. Is that a concern for you?

Mike Haley: Yes, it is, as a taxpayer and one who wants to see precious resources going into front-line services, whether that is health, housing or education. The NAO stated that £15.7 billion has been lost to fraud just on the Covid-related schemes, let alone in the normal day-to-day fraud without Covid. We are talking about billions of pounds.

I used to be head of fraud at the MoD, and £15 billion was what we spent on defence procurement. That is our whole defence budget investment. You could double that if you wanted to, and we might need to. It is certainly a concern. What is not talked about enough is where the money is going. That £15 billion went to criminals and dishonest people. Do we want the type of society in which they just get away with that scot free? Criminals use that money to fund other crimes, such as people trafficking and drug dealing. There are well-researched connections by the Royal United Services Institute demonstrating the links between crimes. Policing needs to understand that. If it understands that more, it will be more about the whole crime problem and not just the fraud problem.

Katy Worobec: I agree with a lot of what Mike has said, as you might expect. I just have a couple of observations. We have our own Dedicated Card and Payment Crime Unit, a police unit funded by the banking industry, which does a lot of work on targeting organised criminal gangs in the UK that are involved in fraud. It has a very good success rate and is doing good work, but it is the tip of the iceberg. To build on what Mike was saying, it would be good to see tougher penalties when people are prosecuted so that it acts as a deterrent.

The final point I would like to make is about the nature of the types of fraud that we are dealing with. There is volume fraud with lots of victims, often for relatively small amounts, not to the victims themselves but in the greater scheme of things. It is extremely challenging for any police force to deal with that. There is certainly a need to focus on how we can better share information and intelligence within the industry, with other sectors and with law enforcement, so that we can more quickly build a better picture of the types of crimes that are taking place, pull that together and focus on organised criminal gangs, rather than trying to

deal with each and every type of crime, which would be practically impossible.

Arun Chauhan: I echo what both Katy and Mike have said, but we should not confuse the police identifying fraud as a low priority and not recognising the impact of fraud on, say, consumers, with the challenge, which they know about from day one when there is a report, of trying to identify and obtain a successful prosecution. Most police forces recognise that finding the perpetrator is very difficult. When a victim hears, "We're not going to investigate this any further", that translates to the victim as, "We don't give credence or value to this type of crime". The police very much do. I have colleagues in the Fraud Advisory Panel and at the City of London Police who I know full well care hugely about this type of crime. The issue is identifying perpetrators and so managing the expectations of the victims when they approach the police. That is being translated as "The police don't care" or "The police don't value them".

Q16 **Lord Browne of Ladyton:** Arun, this question is directed first to you, if I may. Your last answer has taken us towards it. We are the Fraud Act 2006 and Digital Fraud Committee, so this goes to the heart of what we are about. The fundamental question is: what is your assessment of the Fraud Act 2006? If I may say, Katy, it is the ultimate deterrent. It ought to be, anyway. There are essentially two aspects to this question, without getting into the detail of them. First, in a digital world, is it an effective legislative tool? Secondly, is its enforcement effective? In cases where there are allegations of breaches of its provisions, is the prosecution effective? If not, why not, and what recommendations could we make to improve that?

Arun Chauhan: My experience as a solicitor is that I deal with the civil side. I do not deal with the criminal side. Obviously, the Fraud Act is a piece of criminal legislation. My honest appraisal of the Fraud Act is that it is a good piece of legislation. It has simplified fraud offences into a characterisation of wide-ranging areas of crime, such as fraud by misrepresentation.

My issue with the Fraud Act is that it is not a good deterrent. I am probably repeating myself; I come back to the proximity between the perpetrator and the individual in the digital age we are now living in. If the predominance of fraud is by tricking people through online means, impersonation and the very good corporate hijack of organisations, the chances are that those perpetrators are overseas. They are not going to worry about whatever piece of legislation we have as a deterrent for prosecution, because they think that the chance of being prosecuted and identified is very low, so it is not really in their equation. That is my honest assessment. The Fraud Act is a brilliant piece of legislation for the prosecution of a more straightforward crime such as a dishonesty offence, an employee stealing from an employer or abuse of position. Where you have a fraudster impersonating a finance house or a cryptocurrency digital exchange, unless they are in our country they are not going to be worried about prosecution.

Is the Act a deterrent? I do not think so. Is it effective for the digital world? It is, if you look at the offence of misrepresentation or fraud by false representation. That is what is happening online. I can think of a client who had been on a very well-known search engine. They thought that because an advertisement for cryptocurrency was on that search engine it had been verified and was legitimate. It had not been. They were duped and lost £100,000. That was fraud by false representation by those posting that advert, so the Fraud Act would work if you could find them.

My view is that it is effective. The issue is that we are not identifying the perpetrators, and the parties who can identify the perpetrators in the digital world are those who are giving them the platform. We come back to the online debate. I know this is not the forum for the Online Safety Bill, but that is where it leads to.

Sorry, Lord Browne, I realise that I did not answer your question: is enforcement effective? Prosecuting fraud is quite difficult. I heard from a couple of barristers who deal with prosecution of fraud and financial crime that they have concerns at times that it is overly complicated for persuading a jury of the offence. The legislation has been simplified; the offences are often very complicated and complex. There has been talk of economic crime courts and even professional juries. That is one barrier to entry that I have heard about. It is difficult to persuade or to help a jury to understand. We might need to give thought to that.

Lord Browne of Ladyton: Given your experience, because I think this is consistent in civil proceedings as well as in criminal proceedings, are you in favour of special courts that are particularly equipped to understand the challenges of this very technical and specialised area?

Arun Chauhan: Yes, in short. We have sleepwalked as a country into this epidemic of fraud. Look at the economic crime plan a year ago. There were 52 action points and only seven were about fraud, most of which were about the public purse. We have allowed ourselves to sleepwalk into a world in which consumers have almost been forgotten about when it comes to fraud. If they want to see a proportionate response and prosecutions, we need specialist people to understand and demystify those crimes. A specialist court would be a positive way forward.

Katy Worobec: If I can just build on that, we would agree that the Fraud Act as it exists is an effective mechanism to combat fraud in the way Arun has described. Because the landscape has changed so significantly, what is lacking—perhaps you might think this is slightly tangential, but it is important—are the powers needed to tackle the types of fraud we are seeing. Although the legislation in the Fraud Act itself can be used, there are powers needed on top of that to help to tackle the types of fraud. We have a landscape where it is very difficult to share information at pace in order to allow the financial sector to manage the risk by slowing down payments. Looking at powers to prevent and tackle cashing out—a tougher stance on mules, money service bureaus and crypto exchanges—

in addition to what the Fraud Act gives us would be a good route to follow.

Mike Haley: I agree. I have been prosecuting under the Fraud Act from almost the time when it came in. It is an effective legislative tool. I would disagree with Arun to an extent. There are many tens of thousands of fraudsters in the UK who feel that this is a low-risk activity, that they are beyond the law and that they are unlikely to be prosecuted. We can up the ante. There is a lack of capacity in the system rather than a lack of legislative tools.

The legislation can be effective in some of the side issues. The Online Harms Bill is seeking to address part of that in relation to the advertising of scams. We have seen the economic crime reform Bill looking at the Companies House legislation reform, which has been a vehicle for company fraud. Things are being done, and I would definitely like to see a more general duty on businesses to prevent economic crime, including fraud. Quite often, and Katy illustrated this previously with the kill chain, there can be parts of the fraud chain where an organisation has no consequences for enabling fraud that is felt somewhere else. If someone enables fraud, they do not suffer the losses because that might be by the bank or the individual later on.

If there was a general duty on that organisation to do everything in its power to prevent fraud and economic crime, and to have a due diligence defence as there is under anti-bribery legislation, there would be some downside to enabling fraud. If I had one wish, it would be for that to drive the behaviours in the right way, as it has under anti-bribery and corruption. As fraud changes, we might find a different player in the kill chain who does not fall under the Online Harms Bill or Companies House legislation. We then start with creating something new rather than there being a duty that you must take some ownership for preventing fraud.

The Chair: We will move on, but, Arun, we are interested in the Online Safety Bill. Lots of other committees have taken evidence on it. If you wanted to add something on that or write to us with anything extra, we would be very grateful to hear from you on that, specifically given your expertise.

Arun Chauhan: Thank you, Baroness Morgan. I think I will do.

Q17 **Baroness Bowles of Berkhamsted:** I am very pleased to hear you mention essentially a failure to prevent fraud. I have had several goes at introducing such an amendment to other Bills in the Lords.

I want to continue, first with you, Mike, but others can also give views, in subjects that have already been touched upon. What is your analysis of the Government's current approach to countering fraud? There are lots of policies, strategies, plans and updates—half a dozen or more of them just last year. Do they do anything? Again, as we have already touched upon, are sufficient resources made available to organisations tasked with tackling fraud? Are they empowered—and alongside "empowered" I

would say incentivised—to do their job effectively? What are the main things that could be done to speed up and make things more effective?

Mike Haley: To the overarching question about whether there has been sufficient government attention to trying to corral the different forces to have a more joined-up effect against fraud, I have to say that there have been stops and starts. I was chair of the Home Office's Joint Fraud Taskforce for two years, and I found that the regular changing of the Security Minister who had the fraud remit meant that we kept starting again by briefing a Minister, seeing what their particular view was, stopping and coming back to it. There were some good Ministers. Damian Hinds now seems to be getting a grip and is interested, so I have become more favourably inclined to put our resources and assistance into the Joint Fraud Taskforce as well.

There has been a lack of tangible outcomes from those types of activities, even though it is the right thing to do, with public and private coming together, common resources and law enforcement tackling the problem. It is not a problem where we just say that the Government and law enforcement do not do enough. It really has to be a joint effort, with the private sector also stepping up to the mark. The private sector wants to fully engage with these types of bodies.

You are quite right that I am sometimes very dissatisfied or frustrated by the number of plans and strategies. There should be a single national fraud strategy that we all sign up to. We can physically sign up to a group of things and say that we would want to put these things into place. We could all sign up to an action plan, with a single place accountable for that. At the moment, I have meetings with the National Economic Crime Centre and the Home Office Joint Fraud Taskforce. We have a group called Stop Scams that has been bringing the private sector together. We have the Economic Crime Strategic Board. It is a very complex environment, and we keep stopping and starting.

We could do much better just from that. Let us have some leadership: "This is the plan. This is our strategy. Get behind it". Then we will put our common resources to good effect. It needs to be properly resourced. This cannot be done on a shoestring. It has to have longevity and it cannot be done on the side of a desk, as it often has been, although I am seeing some progress in the Home Office on better resourcing of the action plans that are coming out. We are moving in the right direction, and we need that sustained with proper resourcing.

With regard to powers and incentivisation, these are very interesting questions. I would like to think more about how we incentivise organisations to do the right thing, but my member organisations and I want to do the right thing. We do not really need great incentives. We just need that leadership and say, "Come along. Let's be open and honest with each other and trust each other to fight this now common enemy and common problem". I do not need to be incentivised to go to these meetings and put my resources to the greater good. We just need better organisation, a long-term view and a strategy.

Baroness Bowles of Berkhamsted: I was thinking more of incentives for those charged with catching the frauds. You have already said that the local police have every reason not to want it on their tab because they know that the clear-up rate is low, it is difficult, they would not necessarily even have access to the National Cyber Security Centre's data and all those kinds of things. How realistic is it to get all that joined up? Should it be a local police thing, or should it always be done as it is at the moment—well, it is not always—from the centre? Is it possible for local police to be involved?

Mike Haley: It is not impossible. There are two schools of thought. One is that the counterterrorism model with the Metropolitan Police lead, delivered locally, has been effective. The other isa centralised force to deal with fraud on a national level that has the capabilities and the interests, where other crimes do not trump it.

I will give you a good example. I was a customs investigator for nine years. We did fraud, drugs and all sorts of prohibitions. If you get up in the morning to deal with a fraud case, and someone calls up and says there is a drugs case, you have to make a decision. Do you let drugs go into the UK, or do you carry on with your fraud case? Most people in authority say that, given the risk there, they are not going to let these drugs come in, so they are always pushing the priority of fraud down.

It needs to be someone's priority. At a local level, it is always going to be pushed down the priority list. It could be a priority only if it was brought into the policing requirement as a priority. That would create the pressure for having to report on it in order to show what was done. Some will argue that that is the best way to go. It is still a local issue. Local victims need to be reached out to and cared for. The more effective route in the long run, although this would take bravery to change the current situation and see it through, would be a national fraud investigation service and specialist skills—what you get up in the morning to do. A mixture of policing, civil accountants, solicitors and others who could take this forward would be a really good idea, but that is clearly a lot of effort and there are examples of just creating a new body not always being successful.

There are two models. If you are going to go with one locally, make it a policing priority. If there is not the appetite for that, this is a global problem that needs to be dealt with on a national level. Therefore, let us bite the bullet.

Q18 **Baroness Henig:** Good morning, everybody. In the first instance, can I direct my question to Arun? Obviously others can come in. It is about what Katy said earlier about sharing intelligence. The problem is surely that there are so many sectors now involved in counter-fraud, in both the public and the private sector. Whose responsibility it is to tackle fraud? We hear about the need for leadership. Which sector is that leadership to come from? How is the co-operation between the public and private sector bodies working at the moment, and what needs to be done to facilitate the sharing of intelligence?

Arun Chauhan: We have talked about data sharing for years in the counter-fraud space. Prosecuting authorities want to get on with obtaining the evidence. I have colleagues in banks who talk about how the general data protection regulations or the Data Protection Act hinders their data sharing or the interpretation of it. Online tech companies, telecoms companies and banks will often get legal advice before they share data, because they are conscious of the potential comeback on them, as crazy as it sounds, from the fraudsters whose details they are about to give away in order to help a prosecution. Data sharing is desired, but it is hindered by fear of some of the data protection legislation.

It is not just government's responsibility to tackle fraud. I have something to say, perhaps for another question, about education. It is across the piece; it is about individual businesses. You have a situation in which you need to have self-policing and a deterrent to ensure that self-policing takes place. I often mention the online safety side. If these tech companies are, for example, allowing an artist on a YouTube channel to sing about how you can commit fraud, scam somebody and contact him to obtain details of how to commit fraud and if you pay £100 to him, the seniority in the organisation that is allowing that on its platform needs to be held to account. Every sector that allows itself to be a conduit or an enabler needs to be self-policed. If that does not work, they need to have a deterrent: "This will be the sanction for you if you do not do it".

I have sat with board members in a range of sectors, and one message has stuck with me for about nine years. I was telling a CEO of a board about the financial crime risk his organisation faced. He said, "Do I need to do something about this?" I said, "Yes, I think you do". He said, "The last thing we need is another centre-led initiative, unless there's a personal risk to me and people on the board".

I do not want to sit here with a battle axe saying that we need to imprison directors and so on, but they need to feel that there is some personal accountability, because until they do they will not drive their product to be safe over profit. That sector responsibility is a real worry. Everything Mike said on the previous question is spot on. We need single leadership and uniformity. The Government are trying to do more. Lord Agnew recognised some of the failings. Individual sectors need to have corporate maturity now and recognise that they need to prevent financial crime just for that, not just to prevent bad reputation or fines. They need this to be part of their mission going forward.

Baroness Henig: How are private-public partnerships working at the moment? A number have been set up. You are almost implying that they are just formal entities and are not making much impact.

The Chair: We are straying into the next question. Lord Sandhurst, why do you not ask the next question? Then we will ask our witnesses to comment on both those aspects.

Q19 **Lord Sandhurst:** Very simply, what is your assessment of the public-

private initiatives to tackle fraud? How are they working? I am looking in particular at the Economic Crime Strategic Board and the Joint Fraud Taskforce. How often do these groups meet? Are they doing anything or achieving any tangible outcomes? Are they just talking shops?

Katy Worobec: The Economic Crime Strategic Board meets a couple of times a year. It is a force for good. If I can look to one particular example recently at the beginning of last year, as a result of the board convening we were able to pull together a round table with the online platforms and techUK through four Ministers coming together. That has led to the setting up of the Online Fraud Steering Group, which I am involved with along with UK Finance. That move from the Economic Crime Strategic Board to the setting up of the Online Fraud Steering Group is a real example of how the convening power of bringing senior people from government, law enforcement and the private sector together with a general focus on economic crime can really make a difference.

There is sometimes a tendency for these things to be too stage managed. We have set up on the back of that a monthly meeting with Security Minister Damian Hinds, the chair of UK Finance and a number of other people from the Government to keep the pace going and to try to deal with things almost in a project-like way, rather than as set pieces from time to time during the course of the year.

If I can point to some of the work that goes on in the public-private partnerships under the National Economic Crime Centre, there are a number of cells of people working together on specific aspects of crime. This is really making a difference. There are some really good examples of these things working. We are very committed to that happening, but they must be active and lead to action as opposed to being talking shops.

Mike touched on the Joint Fraud Task Force earlier, and I tend to agree with his opinion. It has been re-galvanised by the fact that Damian Hinds, as Security Minister, has taken the chair, but it is still early days for that. The Government can make more use of their convening power to bring together the sectors that do not necessarily have skin in the game and to get them to step up to the plate. They can also take responsibility for ensuring that we have the right powers to enable the sharing of data. It is not just on the data protection side; it is also about putting powers in place to help prevent money laundering. The following of money and the repatriation of funds are being hampered in some ways. These are the sorts of things that public-private work needs to be able to tackle.

Lord Sandhurst: That is very helpful and encouraging. Could you give us a couple of examples of practical outcomes—in other words, things in the last 12 months which the committee has said, or people have realised, would be a good idea and which have started to take effect?

Katy Worobec: If I build on the Online Fraud Steering Group, which I mentioned as coming out of the Economic Crime Strategic Board, we have been working with the tech sector and online platforms such as Amazon and Google. The first thing they have done is to commit $1

million of ad credits to support our Take Five education and awareness campaign. We were working with them to get those on the platforms. There is definitely a willingness and an ambition to make things happen. I should not underestimate the amount of time it takes to build trust and confidence between sectors to really get things moving, but there have been some real moves in that space. That is a really good example of something that has come out of one of those public-private bodies.

Mike Haley: I have one specific example. Under the Joint Fraud Taskforce, a number of charters for different sectors have been drawn up to see whether certain activities could be agreed. There are ones for banking, telecoms, accountancy and law. Again, I agree with Katy that it is too early to see what impact they are having. One example would be where the accountancy bodies started thinking about their role in identifying fraud. I was invited to a meeting of the executive of the Chartered Institute of Management Accountants. It started a discussion about its role in identifying fraud in business and preventing fraud. That leads to the start of these discussions, which then start flowing into different organisations. We are in the foothills but going in the right direction with some of these bodies now.

Q20 **Lord Allan of Hallam:** As this is my first appearance in a public session, I declare an interest that may be relevant to the work of the committee. I am an unpaid non-executive director at the Centre for Public Data, a community interest company.

This question is directed primarily at Katy Worobec and builds on the conversation we have just had about the Online Fraud Steering Group. It is really to dig into whether there are specific obstacles facing the financial services sector in doing more to tackle fraud, particularly in relation to your connections to the telecom and tech companies. Could more be done to improve your ability to work with them to tackle fraud?

Katy Worobec: If I look at the work that we have done with the telecoms industry in the recent past, before the Online Fraud Steering Group was set up, we had been working quite successfully building a relationship with the telecoms sector. As a result of that, we have been able to put some work in place to crack down on number spoofing—the practice of phone numbers from trusted organisations being spoofed, and then duping people into thinking that they are talking to somebody they are not—and with text message providers and law enforcement to block scam text messages in a similar vein. As I said, it takes a good amount of time to build that level of trust, confidence, and indeed understanding between the industries. With the online fraud and platforms, we are at that earlier stage of mutually understanding the problems and vulnerabilities on each of the platforms—they are different; there is no one-size-fits-all solution—and, from there, how we can mitigate the vulnerabilities that are being exploited by the fraudsters.

On the barriers and obstacles to that, and getting past the trust and confidence piece, again I go back to the information-sharing powers. We would like to be able to share information between the sectors, as much

as anything, to see what we can do with information if we can share it. Can we build and mitigate against fraud as a result? We need the confidence to do that. There are data protection aspects but, as I have said, it is also about being able to feel comfortable that the powers that are there will adequately cover the sharing of data at pace.

If we can get past some of those barriers, it may just be perception, but in some cases we might need some kind of comfort, if you like, from regulators or government that we can do this, even if the legislation might be a longer-term thing. There could be a degree of comfort that says, "It's okay to do this. Feel that you can". That would help people to feel more confident in sharing information between the sectors.

Lord Allan of Hallam: It seems that the fraudsters share information with each other. If those fighting the fraudsters cannot, there is a problem. I do not know whether anyone else had a thought on the priority they would place on information sharing and resolving that.

Mike Haley: You would expect me, running the largest data and intelligence sharing organisation with 600 members, to say that that is probably the biggest priority. We voluntarily share t data and intelligence, and we do that under GDPR and the Data Protection Act. It is in the legitimate interests of businesses to protect themselves, and we have a number of bodies now joining the organisation, including 30 local authorities, mainly because of the impact of the Covid grant schemes and seeing that they were also being attacked. The legislation is there; it is about the confidence that the regulator is not going to come after you if you start sharing information and intelligence to prevent fraud.

We have talked about the scale of fraud. To tackle it will be about prevention. We have to put most of our effort into preventing fraud happening in the first place. We have spoken about the need for a deterrent. We can prevent fraud the most by sharing intelligence at the right time and sharing information under a framework where everyone has confidence to do that. The ICO is moving with its sandbox approach, and that could go further to say, "Look, there's this legislation. There obviously have to be certain balances and mitigations to ensure that the privacy of individuals who are not fraudsters is protected".

There are some good examples under the Digital Economy Act that allow public bodies to share under certain conditions. Why not look into why that cannot be public to private and private to private? The mechanism is there, and it has lots of checks and balances in it because it is a balance. We do not just share everything. We have to be really proportionate about what we share, and there has to be a very good reason for it. We are happy to do that. It is confidence, more than legislation, that is needed.

Q21 **Baroness Taylor of Bolton:** Can we move on to victims? Arun has mentioned consumer education, Katy has mentioned the weakest link, and we have talked about personal responsibility. There has been quite a lot of effort to educate consumers through different campaigns or

television programmes. I phoned my bank this week for the first time in a long time and got a little lecture on some of the scams that might be directed to me, which was very useful for lots of people.

How do we target people in an effective way to get them to really understand what might be happening to them? Are there examples of successful campaigns? What is the best way of going about this?

Arun Chauhan: I will come on to the effective campaigns. The Take Five campaign was quite successful. Perhaps just indulge me for a moment with where I am going with this. My view on education is that if you are going to educate and try to help people to prevent fraud, your audience needs to be mindful of the fact that it is at risk. I am not sure that society as a whole thinks that it is at risk of fraud. Only a few years ago, people would think that fraud was one of those stories they would read in a paper or online and that it would never happen to them. I am not sure that we have a fully receptive audience to all the very good messaging that goes out.

We need a generational mind shift and change. It is akin to road safety. This isn't angling to very young children, but my nine-year-old son came to me the other day and said, "Someone tried to scam me today". One of his friends tried to trick him. He understands the lingo. He hears me talking. He is bored of me talking at home, no doubt. He knows to look both ways before he crosses a road and that I should wear a seatbelt when I drive.

One body that we have not talked about that should be involved in this dialogue is the Department for Education. From year 8 or 9, children need to understand what fraud is. There are three reasons. First, they will talk about it at home, so parents will start to hear about it. Secondly, they will learn about fraud and the implications of being involved in it. They will be aware of the deterrent of the legislation, so they are aware of the wrong side of fraud but also how to protect themselves. Thirdly, we often ask our employees to be our eyes and ears in our organisations to help to detect fraud and whistleblowing. Whistleblowing is not as significant as it should be in England.

People know what fraud smells like, feels like and can be, and that is part of their psyche growing up. They will know to look both sides of the road before they cross. They will know to wear a seatbelt. I would implore us, if anything from today, to look at the campaign to help to educate younger people, because that will put us in a better position in 20 years. So far, in 20 years, I do not think we have moved that far in fraud prevention. I will leave it Katy and Mike to talk about the campaigns that they have been directly involved with more than I have.

Katy Worobec: We spoke about the Take Five campaign earlier. I do not disagree with what Arun just said. It is important to have a consistent set of messages at a high level. The problem with these types of frauds is that fraudsters are constantly changing the way they work, as we observed earlier, so it is important to have a high-level message. It is a

bit like the "clunk click" thing, if we use the seatbelt analogy, or Take Five, which is "stop, challenge, protect". It is those key messages that you can then use flexibly to talk about whatever type of fraud or target audience you want to focus on. It is important to have that background and to have that reinforced all the time.

Through UK Finance, 33 of our members are signed up to the Take Five charter, which means that they are taking the messages of that campaign and using them on their cash dispensers, statements or websites, so they are constantly reinforcing the messages of that central campaign.

That needs to be complemented, though, and this is what is happening as part of the push payment voluntary code. There needs to be more effective, targeted warnings and advice to customers at the point at which they are going to make a transaction. Someone mentioned that their bank lectured them slightly when they phoned them up, so there is an example, perhaps. Certainly when I go into my online banking, I see warning messages saying, "This is a type of scam. Are you sure that this is not a scam that you are dealing with?"

You need the general background and the very targeted warnings at the point at which the transaction is made. Although educating young people is vital, there is a sense that we can all be vulnerable, in its widest sense, at any given time. Somebody who is recently divorced might be vulnerable to romance fraud in a particular way. We have to keep flexing any education and awareness campaigns to target different audiences and different types of scams. That is why that Take Five umbrella campaign is really powerful. You can then use it to target particular audiences and particular types of scams.

Baroness Taylor of Bolton: How do we stop being paranoid? When the bank phones you to say that it has detected an unusual transaction, how do you know that that is not another scam, when it is genuine?

Katy Worobec: I agree. The problem is that we do have to be slightly paranoid. I certainly take none of these things at face value. The answer is simply to empower the victim to say, "You say you are my bank. I'm going to put the phone down and call my bank on a number I know".

Baroness Taylor of Bolton: They use a different number.

Katy Worobec: Yes, take the power back. This is the UK. We are still all very polite to each other. We need to go, "Fine, I'm taking my power back now. I'm going to contact my bank and confirm that you are who you say you are". Anybody who is genuine—it does not matter who it is—and not an impersonator will know that that is the right thing for the victim to do.

Baroness Taylor of Bolton: Can I just go back to Arun on education and young people? The point he was making was very good, because lots of grandparents get their grandkids to tune the television or whatever, so that is a really good way in. One of my colleagues was talking about

students who become money mules and get drawn in. Is there any way we can alert people in that situation, who may be financially challenged, to be more aware?

Arun Chauhan: Part of my thinking about the education starting at, say, year 9 is that if children in year 11 are going to be able to access a bank account at 16, they are warned prior to then about this. It is part of the education programme in well-being or whatever section of education it is, but they are warned and it can be reinforced. Of course, lots of people leave education after the age of 16, so it is about understanding what the avenue or the route is to educate them. If they do not stay in the schooling system—college or university—we should not exclude that part of society. Everyone needs to hear it. That is why I thought about school years 9 to 11. That will capture the majority of our adulthood in this country for years to come, and that is the best place for it.

Lord Sandhurst: Are you not starting quite late at that stage? I would have thought that children aged seven, eight or nine are quite capable of taking simple concepts on board. Certainly with road safety they do. Should we not be starting earlier, right at the very start, and then developing it as it goes along, so that it just becomes part of the culture? That will then feed back into the homes, because they will tell mum and dad.

Arun Chauhan: Absolutely. We would love that to happen. I thought I was being overly ambitious by going into a junior school. I mentioned my nine year-old. He talks about scams. He understands tricks. He clearly can get it. He has his mum's intelligence, not mine. All children of that age are sponges. They want to learn. It is an interesting thing to learn about. Maybe this is slightly high-level, but we should not all assume that everyone's moral compass points due north. People understanding what right and wrong is from a younger age is possibly a good thing. If we can get it into a younger schooling system, I would completely endorse that.

Mike Haley: Arun might not know this, but it addresses two things. First, what type of activities come out of the Joint Fraud Taskforce? There are lesson plans for key stages 1 and 2 developed with the PSHE organisation and with educators to be part of the curriculum, but whether those up-to-date PSHE lessons are utilised is a choice. They have been developed with policing and with organisations like Cifas to give the right types of message at key stages 1 and 2, but they are not mandatory. This is a life skill that is about managing your own money and how you can protect yourself from fraud, as well as about how to not get involved in fraud.

It is quite easy for young people, as you point out, suddenly to be told, "This is just flipping your cards and your account. It's easy money and you need it", while it is laundering the proceeds of crime. People are not realising that. These lessons have been developed around identity fraud and money muling. They are there. This year, we have been asked whether we want to update them, which we are going to agree to with the PSHE organisation. They have been used in about 2,000 schools, but it is a drop in the ocean.

There are certain areas and schools where we know that there are young people called 'fraud stars' who will hang around the gates and recruit people—we call them mule herders—into money mule activity. They have a whole lingo about it, such as "squares". If you have a certain colour square, that might be a Santander card or whatever. If you do not realise that this is criminal activity, and what the repercussions and consequences are to protect yourself, we will end up, as Arun mentioned, sleepwalking not just into an epidemic of fraud but into our young people seeing it as a legitimate way of getting a new pair of trainers or a bit of cash. I would argue that we have gone so far but we could go that bit further to make it a mandatory part of the PSHE curriculum, because it is a life skill.

Q22 **The Chair:** I have one final question, which Mike has already pre-empted, so I will see whether he might want to change his answer. My question then is to Arun and Katy. If there is one policy recommendation that you wanted to leave us with, what would it be?

Arun Chauhan: I am grateful to Mike for mentioning the lessons. I would ask that they are made mandatory. That life skill is part of everything. I fully echo what Mike has said. That would be my recommendation.

Katy Worobec: It is to provide a legislative vehicle so that firms can take a risk-based approach when they are processing payment transactions. It is about the ability to hold or slow a payment where the firm believes that the customer is at risk from fraud, and creating that legal framework to follow the stolen money through the system and to freeze it before the criminals can cash it out. We have the technology that allows us to follow the money, but the legal framework is not there to allow us to do anything about it. That is what I would ask for.

The Chair: Mike, your recommendation to us earlier was about the enabling of fraud and focusing on that. Is it fair to take that as your recommendation?

Mike Haley: Can I be cheeky and not change my mind but add one? We have not talked much about one of the biggest fraud issues in the last year around things like bounce-back loans. We found that industry standard fraud checks that have been used in banking for a long time were not utilised, and we did not have good sharing between big organisations such as DWP and HMRC, which sit on tons of fraud data, because they are attacked all the time. Why oh why can we not get that shared with the rest of the sectors to help protect UK plc and get out of this siloed thinking? It would be a dream for me that we just have public and private data sharing to prevent fraud because it harms UK plc. Let us do something about that, please.

The Chair: I do not mind you being cheeky, Mike, because you set it up very well for our next witness, Lord Agnew. Can I thank all of three of you very much indeed for your time this morning? We are very grateful.