HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Fraud, HC 125

Wednesday 17 January 2024

Ordered by the House of Commons to be published on 17 January 2024.

Watch the meeting

Members present: Dame Diana Johnson (Chair); James Daly; Tim Loughton; Alison Thewliss.

Questions 73 - 148

Witnesses

I: Mike Haley, Chief Executive, CIFAS; Richard Hyde, Senior Researcher, Social Market Foundation; and Sophie Davis, Director of Research, Crest Advisory.

II: Professor Nicholas Ryder, Professor in Financial Crime, Cardiff University; Professor Nicholas Lord, Professor of Criminology, The University of Manchester; and James Babbage, Director General of Threats (Economic and Organised Crime), National Crime Agency.

Written evidence from witnesses:

– [Add names of witnesses and hyperlink to submissions]

Examination of witnesses

Witnesses: Mike Haley, Richard Hyde and Sophie Davis.

Q73 **Chair:** Good morning. Welcome to the Home Affairs Select Committee. This is our second session in our inquiry into fraud. The aim for this session is to understand the prevalence, scale and nature of fraud in the United Kingdom, to examine whether the Government's plans are effective enough to protect people from fraud, and to explore the cross-cutting nature of fraud and its links to organised crime, including serious corporate fraud and terrorism. We have two panels this morning and I am very pleased to welcome our first panel. Could the panel introduce themselves? Would you like to start, Mr Haley?

Mike Haley: Thank you, Dame Diana. I am Mike Haley, the chief executive officer of CIFAS, a not-for-profit membership organisation. We run the national fraud database on behalf of the 700 members of the organisation.

Richard Hyde: Good morning, everyone. I am Richard Hyde, a senior researcher at the Social Market Foundation. We are a think-tank based around Westminster and have been going for 30-odd years.

Sophie Davis: Good morning. I am Sophie Davis. I am the director of research at Crest Advisory. We are a consultancy and think-tank dedicated to improving the criminal justice system.

Q74 **Chair:** Thank you. We have a number of questions for you, but it might be a good place to start if you could paint us a picture of the current trends in fraud, the methods being used, and the types of fraud that are being committed in the UK, dealing with the last few years in particular, and whether there have been changes. Ms Davis, would you like to start?

Sophie Davis: The first thing is that there has been a huge rise in fraud in the last 10 years. In the year to June 2023 there were more than 3 million offences, compared with about 230,000 in 2013. That is an exponential rise in fraud. It has become the most commonly experienced crime in the UK, and now makes up about 40% of all crimes in the UK. There was a shift to high-volume, low-value fraud, driven partly by our move online and the digitisation of our lives, and enabled by technology such as bot communications and number spoofing, which have allowed fraudsters to carry out fraud on a much wider scale. The increase has been driven in large part by authorised fraud. There is still a huge amount of unauthorised fraud, but we can see that the rise has been driven a lot by authorised fraud.

Q75 **Chair:** What does that mean?

Sophie Davis: Authorised fraud is, in a way, authorised by the victim. The fraudster tricks the victim into authorising a fraudulent payment, as opposed to unauthorised fraud, where the fraudster uses the victim's bank details, for example, to carry out the fraud.

Some factors that have contributed to that rise are, as I said, digitisation and the move online, which have also enabled more fraud to be committed from overseas. We now know that about 70% of fraud is committed from overseas. The attractiveness of the UK market is a factor. The English language and the fact that we were an early adopter of the faster payment system makes us a very attractive destination and, combined with the move to online, enables overseas fraudsters to take advantage of that. Also there has been deprioritisation of fraud. Over the last decade a lack of enforcement from policing has created a bit of a vacuum there, which has allowed fraudsters to take advantage of it.

Q76 **Chair:** Say a little bit more about not pursuing fraudsters. Are you saying that the UK is not at the forefront of pursuing perpetrators of fraud?

Sophie Davis: Yes. I think fewer than 1% of frauds that are reported are charged and prosecuted. That creates a bit of a law enforcement vacuum. Because of the structures in which it is set up—the architecture of fraud, but also the capabilities and resources in policing over the last decade—the police have not really had the capability and time to go after fraud as much. That creates a bit of a vacuum for fraudsters.

Q77 **Chair:** That is very helpful. Thank you. Mr Hyde, is there anything you would like to add to that?

Richard Hyde: Not too much. It was a pretty comprehensive summary of where we are.

Chair: Okay.

Mike Haley: Perhaps I can take a slightly different direction around the fraud types that our members report to us. Last year we had a record year, with 409,000 cases reported by our 700 members to the national fraud database. That is about 1,000 a day. Over the last 10 years we have seen an inexorable rise. It is quite well known that other acquisitive crime has reduced and as that has happened it has gone into fraud. We have seen an increase in scale and sophistication.

In terms of scale, it is not just scams. We are in danger of equating all fraud with scams—the authorised push payments that Sophie spoke of. It is very well known, because there is a big impact on the individual; but 68% of those 400,000 cases involve identity fraud. The loss in identity fraud tends to be to a business, which could be a credit card issuer, bank or insurer, but it also impacts on the victim whose identity has been stolen. Identity fraud has been going up about 10% each year, and 88% of it occurs online. The pandemic increased everyone's online engagement, and now we see that in an increase in identity fraud.

We have seen an increase in what we call facility or account takeover. This is a more sophisticated crime, where organised criminals tend to get our credentials—our passwords, the emails and phone numbers that we set up, and credit card and bank accounts—and take them over for their own use. Even this morning I woke up and, on going to Facebook,

realised that there had been an attempt to take over the Facebook account. Friends quite often say, "Ignore everything that is on your Facebook, because the account has been taken over." That becomes a precursor for getting other information, such as credentials and passwords, to take over accounts. It has all the hallmarks of an organised crime attack, as does identity fraud.

The third area that we have seen, which is less talked about, is first-party fraud. Individuals have become more fraudulent over the years. We see this from behavioural research. In first-party fraud, individuals, for many reasons—it could be for economic reasons or more generally seeking to get something for nothing—make false applications for valuable goods and services. Our online retailer and telecom members see that.

My main point is that fraud is not just about the scams, which have increased, and have a high profile. Identity fraud and account takeover have increased, as have false applications by individuals. There is a multifaceted increase in fraud, across a number of fronts.

Q78 **Chair:** I suppose what you have described there is changing and evolving over time. We have had a lot of debate, recently, about AI. Could you say something about AI and how it might impact on fraud? Will it change the direction of fraud?

Mike Haley: I can certainly kick off on that, because the use of AI-generated content in a number of ways is not a future fraud threat any more, but an existing one. We see it in phishing scams, where people get emails purporting to be from a reputable organisation, whether that is Amazon, DPD or the Post Office, saying that they are going to deliver something and that clicking on a link will give information. It can be more sophisticated, because AI tools make the texts and emails much more similar to the genuine ones that you would get from a company. In the past, individuals were told to look out for poor spelling or grammar in the email, or whether it looked a little fuzzy. Now the emails are more sophisticated, and they are a precursor to getting someone's information. That has become more prevalent.

We have started to see image and video cloning of individuals in scams. Previously someone might impersonate your son or daughter in a WhatsApp family scam, saying, "I need some money. I'm stuck somewhere and I've had to change my bank account or mobile number." We are starting to see voices and faces being cloned, which is far more persuasive to the average person. The onboarding checks for our banking members in particular are being evaded by the use of face-swapping and other types of technology to pretend to be someone else.

There is more sophistication, but it has been going on for a number of years—for example, with SIM swapping, where someone gets access to your phone, and interception of one-time passwords, which were security measures brought in by banking members in particular. We have seen the increase in sophistication, and the fear is that that sophistication

around using AI tools will make it more difficult for individuals to spot what might be a fraudulent attempt.

Q79 **Chair:** Would anyone like to add anything to that?

Richard Hyde: To echo that a bit, we picked up, while doing a report that we published late last year, that there is already a tool that criminals can use called FraudGPT, which will write the spam emails for you in a more sophisticated way. That development of AI is part of the wider system of crime as a service. A criminal does not necessarily have the in-house capacity, shall we say, to do the fraud, but buys in the services on the dark web.

Chair: Okay, thank you.

Q80 **Tim Loughton:** The more we have progressed with this inquiry, the more our brains hurt, because of how big the issue is, how it is growing, and how multifaceted it is, as Mr Hyde said. We have had evidence on everything from romance fraud, which was quite an eye-opener, to terrorism fraud and everything in between. As Ms Davis said, fraud is now 40% of crime, so it is huge.

We do not hear so much about the people behind it. It seems to have gone from individuals chancing their luck to much more sophisticated things. In the old days it was a message originating in Nigeria offering billions of pounds in return for paying 500 quid into some bank account, saying you had been mentioned in a will. It was very unsophisticated. Now, with the use of AI, they are impersonating people you know. AI can presumably be used to try to crack passwords and such things as well, which is really worrying.

Who are the people behind it? Is it now, much more, an organised professional crime gang with laboratories processing all this stuff? You say that 70% is from overseas, but who is behind it in the UK, based on the too few people who have been prosecuted? What is the profile of the people behind this?

Mike Haley: To be honest, I don't think we know enough about who is behind it. We see the footprint of organised criminality, in the sense that sophisticated tools have to be used, and the attacks are at scale. Making applications using people's identities needs the whole train of how you get the identities and utilise them. There are different tools, including using bots and networks of computers to make applications against, say, a credit card company at scale, which is not consistent with an individual having all those techniques, and then a kind of breakdown.

Interestingly, a recent investigation by the National Crime Agency and the Met police, Operation Elaborate, started to reveal the sophistication. There are UK and international criminals in a dispersed gang. Often organised crime is not in the mafia style that we have in our heads. It can be a loose connection between individuals who do different parts and run different services for other criminals. It is quite sophisticated. They

advertise their services online. Some of that is on the surface web; it is not just on the dark web. There is a loose connection of all sorts of people with different skills, whether cracking passwords, sending phishing emails or being able to launder the proceeds. We do not do enough, mainly because, I think, until recently there had not been enough investigations to reveal the techniques. There needs to be more deterrence, but understanding how this works and who is behind it is as important as putting people away.

To Sophie's point about 70% having some footprint overseas, there tends to be a footprint in the UK as well. Some organised crime gangs will be in the UK. It depends on the type of fraud. One issue about fraud is that it is so broad and multifaceted. Cash for crash insurance scams, where people deliberately drive into you and claim, are an organised fraud based in the UK, but some of the proceeds may be laundered overseas. Some of the identity fraud may well be coming from threat nations, or organised crime elsewhere—Albanian, Ukrainian, you name it; there will be people involved, and it may have a smaller footprint. In short, I don't think we know enough. We need to know more to be able to put our defences in place.

Tim Loughton: Why don't we know more? Perhaps that question would more fairly be put to the crime agencies when we have them as witnesses. I had a really interesting instance of a constituent who was defrauded of several hundred thousand pounds. This was a smart businessman, who thought he was paying for a rather racy car, which turned out not to be the case. He paid a six-figure sum into a bank account. Extraordinary. But that bank account had to exist. It was a UK bank account.

Given the complications for any of us trying to set up a new bank account and having to prove our identity, for all sorts of money laundering reasons, you would have thought that there would be a fairly easy trail to who was behind it, yet the bank was unable to provide evidence of who had benefited from the money. It went straight into the bank account and out.

Why is that happening? Surely that intelligence, which is down to money laundering, means that the bank has a duty to be assured that it is dealing with a real human being, and to know who that human being is and that they are a bona fide human being allowed to have a bank account in the UK. How is that sort of thing not a major source of information to track the fraudsters? Most of it involves money going into an account to pay for services or goods that turn out not to be what they are made out to be.

Sophie Davis: I completely agree with Mike that we do not have enough evidence on this, but that the evidence that we have anecdotally points to organised crime. A study in 2018 suggested that about 40% of fraud has some link to serious organised crime. Part of our research to come—sadly, we have not done it already—is to look at the profile of offenders

in particular. We will be doing that later in the year. Part of the problem is the lack of data sharing, and we may come to that later. Data is diffuse across a number of organisations in the public and private sectors. There are some efforts to share data, but it is not as co-ordinated as it could be, and maybe there has been a bit of a lack of drive to collect the required intelligence and share data between agencies, to enable us to see trends and patterns, and to understand.

Q81 **Tim Loughton:** Why? Given that it is 40% of all crimes, and everybody has some experience of fraud, which is a serious cost to individuals and a serious cost to corporations that gets passed on to customers as well, there must be a priority interest in sharing information and working together. Why on earth is it not top of the priority list for the law enforcement services, and all the agencies involved?

Sophie Davis: There are a number of different actors across what is commonly called the fraud chain, from Government to the telecoms industry, online firms, and the banking industry. Some of them are less incentivised than others. The banking industry has done quite a lot, as there is a lot of incentive to act. There may be less incentive for other actors across the chain. At the Government or law-enforcement level I would say the responsibility is quite diffuse. Even though the Home Office is the lead Department, there are a number of Departments that share responsibility. At law enforcement level it is similar. That diffusion of responsibility has contributed to the creation of a bit of a responsibility vacuum, as has, potentially, the lack of incentives for some of the actors across the fraud chain.

Q82 **Tim Loughton:** Who should take responsibility? Who should be co-ordinating everybody? Where does the buck stop?

Sophie Davis: Ultimately with Government, I would say; and then getting all the actors together and incentivising and making sure that there are consequences for actors across the chain who do not share data and take action.

Q83 **Tim Loughton:** Who is the Minister for fraud?

Richard Hyde: Tom Tugendhat.

Q84 **Tim Loughton:** It comes under security.

Richard Hyde: Security Minister at the Home Office, yes.

Q85 **Tim Loughton:** Finally, can I touch on terrorism fraud, which is probably one of the most worrying forms? It is everything from the issuing of passports fraudulently to raising money through various fraudulent means in the UK, which goes to arms or whatever it may be. How big an issue is that, and how sophisticated is it? Anyone keen to answer?

Mike Haley: There are some well documented case studies where money from fraud has gone into the hands of terrorists and funded terrorism. The amounts do not need to be very high to fund terrorism, so tracing it

can be quite difficult. I think our colleagues from the National Crime Agency and Professor Nic Ryder will probably have a more in-depth answer about that, and the links, but, if I may, I will answer a couple of your previous points.

On the money laundering aspects, I see fraud, cyber-enabled fraud and money laundering as a continuum, because people always need to launder the proceeds of their fraudulent crimes. Your question is a very good challenge. Given how difficult it is for the average citizen to set up an account, why is there not much better control? How are they using those accounts?

Over the last few years we have seen a change from fraudsters setting up accounts that they control directly. As the barriers and the checks in place have become more difficult, as we all know from opening our own bank accounts, they have turned to what we call social engineering, which is persuading, manipulating or bribing people to allow them to use their account. They have passed all the "Know your customer" and due diligence checks. Many are students. Plenty of Chinese students allow their accounts to be used for particular frauds. There are other students and young people, but now people across lots of demographics allow their accounts to be used for money laundering.

They may be unwitting, where someone uses a ruse to approach them. We call them money mules. They are like drug mules but they carry money through the system. They have organisers—mule herders—who control a network of accounts and people who set up accounts. The incentive is that they may be paid a percentage of the money that goes through their account. It is kind of short term, until they are found out and exited from the banking system.

Now, with faster payments, the money comes into a mule account and they are instructed to transfer it immediately to another account, which then disperses through multiple accounts and generally either goes to ATM cash-outs very quickly, or overseas. Faster payments make it more difficult to track that and intercede quickly. The success, in fact, of the checks that are in place to make it more difficult for criminals has meant that they have changed their technique.

Q86 **Tim Loughton:** I understand. The mules are guilty of an offence, aren't they? They are aiding and abetting, or whatever it would be.

Mike Haley: Yes.

Q87 **Tim Loughton:** Have many people been prosecuted on that basis? Many people may not realise that they need to do better checks before they agree to that.

Mike Haley: Not as many as I would like to have been prosecuted. There have been some, and there are initiatives around cease and desist. It is sometimes difficult to prove whether someone was witting or unwitting. However, there is an offence; whether you are witting or unwitting, it is the offence of money laundering. Many of the people could be young.

They might be naive and gullible. Others absolutely know what they are doing, and evidence of that is one of the biggest issues.

One of the biggest issues for our banking members is exiting customers who may well have been duped, and who might then find it difficult to get further banking facilities. By sharing more intelligence and data you can see if someone has used a pattern. Are they more witting? In fact, the Economic Crime and Corporate Transparency Act 2023 will allow more sharing between private organisations around suspicions of financial crime, which I think will help in detecting those who do it wittingly, and those who might well be a one-off. Absolutely, it is an offence. We need to make people more aware that if you do this it is not just fraud. You are funding or helping to fund the proceeds of human trafficking and drug dealing. Money muling has more than just a fraud impact.

Secondly, on the question of data sharing, which I think is the nearest we have to a silver bullet in this area, we have so much information, particularly online, around the factors that are being used, whether they are devices or IP addresses. It is about how we can share that quickly between the public, the private and law enforcement, and get that right, including social media companies, who are outliers at the moment and do not share data. For example, there are none of those organisations among our 700 members. Banks and telecoms—100%; but no social media companies, and that is where some of these frauds start. It might have been Facebook Marketplace where your constituent saw what he later found out was a fraudulent advertisement for a car. Lots of car advertisements are fraudulent, because you can get a large amount of money.

Why isn’t sharing data done as much? There is a lack of incentive for some organisations. Facebook, or Meta, are not losing money from fraud. They are making money from organisations and individuals who put posts and adverts on. How do we make the right incentives to share? The banks know they should be sharing. I think we are on the cusp. There is something called the economic crime data-sharing strategy under the economic crime plan, where there needs to be a fraud data-sharing strategy; it is under the Home Office, and we are working towards being able to share more between public, private and law enforcement. From the perspective of the private sector, we want to be able to prevent and disrupt, and get the information about which accounts, email addresses and phone numbers are being used, close them down and then pass the information that we have around crime to the National Crime Agency and the police, for them to do more.

We have a suboptimal system but we are moving in the direction of a more effective data-sharing scheme. Some of it has been around legislation, some of which has already come in, such as the Economic Crime and Corporate Transparency Act. That and the amendments to the Data Protection and Digital Information Bill are starting to give us and

industry more confidence about sharing information without having civil liability for it, such as when sharing information about fraudsters.

Q88 **Chair:** I am going to call Alison Thewliss next, but I want to check something with you. You said something earlier about Facebook accounts being taken over and you have just said that social media companies don't share data at all. Do they take appropriate action when Facebook posts are taken over? Are they doing that bit, or are you saying that they are not even doing that?

Mike Haley: I think they would say they are doing an awful lot to bring down sites, and they probably are, because it is on a huge scale. Close one down and another will be opened. What they are not doing at scale, and as part of established regimes, is sharing the information around fraudsters and the accounts and credit cards they have used to set up accounts. They are an outlier part of the community in sharing in an industrial way. There are a few pilots going on but it is quite slow to get them to be really part of the counter-fraud community.

Chair: Thank you very much.

Q89 **Alison Thewliss:** I want to ask first about the impact generally of fraud on victims and protecting against fraud. Why might fraud victims be more reluctant to come forward or take longer to report their experiences than other victims of crime?

Sophie Davis: First of all, there is a common misconception that the only impact on victims is financial. In our research we have seen that, although there is a large financial impact, there is also a large emotional and psychological impact. A number of victims in our survey said they had experienced anxiety and psychological impact as a result of being a victim of fraud, and a number of them ended up using victim services as a result.

On your point about why victims are more reluctant to report, there is a large amount of under-reporting in fraud. Something like 86% of fraud goes unreported. That is high even compared with similar crime types, like theft, and quite a lot higher than other crime types. There are a number of reasons for that. One is that victims will report, in a way, by telling their bank. That is not reporting for the purposes of law enforcement, but they tell their bank. In the survey that we conducted the majority of people—about 42%—told their bank. Some of them assumed that the bank would then go on to tell law enforcement and that it was no longer their responsibility.

There are a number of other things. One is the very specific nature of reporting fraud, with Action Fraud as the national reporting centre. Many people are not aware of Action Fraud or its role and how to report. The fact that there are different ways of reporting, between Action Fraud and the police, confuses people. Some who have reported say that they get passed around between agencies, which is in a way even more confusing

and upsetting for them. Many people in our research said that they do not think it is worth the hassle. By the time they have recovered their money from the bank they do not see the value for them in reporting it to Action Fraud or the police.

A lot of people express feelings of shame or embarrassment. There is a wider perception in society that victims are partly to blame for their own victimisation. They worry that the police or law enforcement will reinforce that when they come forward. We have actually heard from victims who came forward to Action Fraud that sometimes they were not treated with the empathy that they should be treated with. They were made to feel like it was in part their fault. That has put them off in future victimisations or put off other victims as well.

Some of the businesses that we surveyed felt that it might damage their reputation if people knew that they had been a victim of fraud. It might impact on their customers. There is also the impact of money. When people have lost less money, they do not necessarily think that it is worth their while to go and report it to law enforcement. When people did report, they told us that the motivation for that was a sense of justice and helping other people, making sure that the fraudsters were not able to continue hurting other people. They said in interviews that, even though they felt it was pointless in their own case, they were doing it from a wider sense of justice.

Q90 **Alison Thewliss:** In Scotland we do not use Action Fraud. We would not get very much out of that as a scheme, and I think we are broadly right to do so given its reputation. Is there any particular difference that you have surveyed in terms of people reporting in Scotland from the rest of the UK?

Sophie Davis: We didn't actually survey people in Scotland. It was only in England and Wales. Sorry, I don't have any information.

Q91 **Alison Thewliss:** That is fine. I was just curious as to the extent of that. You talked about the police response when people report fraud to them. Was there any response in terms of people not feeling that the police knew enough about how to deal with fraud? If somebody is assaulted in the street, the police have a very clear understanding of how that crime is recorded and then prosecuted. The nature of some of these frauds can be quite sophisticated. Do they have enough experience in the police? Are they able to direct people to the right place in order to follow up that crime?

Sophie Davis: That came up in our survey and our interviews with victims. Some of them lacked confidence in the police. They did not think that the police would have the right skills and capability to be able to deal with it, or the resources. I think people extrapolate from their experience with other crime types, where very often the police do not have the resources and capabilities to investigate all crimes. At the moment, a very low proportion of crimes gets investigated and charged. If people

take their experiences from that to fraud, they might think that the police would not take it any further. That was reported to us in our survey.

Q92 **Alison Thewliss:** In Scotland we have the Crime Campus at Gartcosh, where they have the Serious Organised Crime Taskforce, so there is a route for crimes to go to people who are specialists within the single police force in Scotland. Is there an issue perhaps of local police forces in England not having the expertise at local level?

Sophie Davis: Probably yes. There are the regional organised crime units, the ROCUs, and part of the new Government strategy is to invest in more expertise, both in the national fraud squad and in the ROCUs. With the cuts to policing, over the last decade in particular, and the number of resources—as an estimate there are about two police officers per 1,000 fraud cases—it is about the time to be able to deal with the number of cases that come to them. There is also the fact that fraud victims are probably less present in the way that a victim of a burglary might be in front of the police officer. They might understand that crime type better, so there might be more incentive for forces to act on those kinds of crimes compared to fraud.

Q93 **Alison Thewliss:** Thank you. Mike, you talked about the issues around identity theft and how that is happening. Do you think it is just criminals in that area finding a gap in the market, where they think they can get in, or is something else going on there?

Mike Haley: Identities are going to be a precursor for lots of other fraud types. We recognise that pretty much all our data has been either breached or lost or has been socially engineered. It is actually traded on the surface web or the dark web by criminals. We need to do a few things there. I echo everything that Sophie said about victims. Identity fraud victims are poorly served. There is a new identity repair kit that the Home Office has put out. We need to make that widely known.

You might be surprised that identity theft itself is not an offence. If I went with a jemmy, glass cutters and a balaclava to someone's house, I could get stopped and arrested for going equipped to rob a house, particularly if I had done it before. If I get details of your identity and I have not yet committed a fraud, I have not committed an offence. There is going to be a review of the law on identity theft because it is now such a significant issue.

There is under-service of identity fraud victims. Sometimes the loss may well be to a credit card company, and you don't lose out, but for a lot of people there is another issue. If you know that someone is going around using your identity, and you then have to pick up the pieces, when your credit score has been ruined and you go on a merry-go-round to repair your identity, there is that kind of impact even though you might not have lost money. Sometimes, someone has to prove that it was not them who took out a fraudulent mortgage, for example, or a credit card

account. The onus is on the individual to sort that out. I don't think that is quite right.

Q94 **Alison Thewliss:** That is interesting. It is definitely something to follow up on around the crime of identity theft in itself. I want to ask a bit more about how people become repeat victims of fraud. Often, it is not just one fraud. They end up becoming somebody on a sucker's list or something else. Can you tell me a bit more about how people can get out of that cycle?

Mike Haley: It is a fraud type called reloading. They even sell the details of someone who has been the victim of a fraud or a scam to others, who might then phone up and pretend they are from the police. They can be very persuasive. For example, if the fraudster knows that on a particular day you transferred a particular amount of money from one account to a fraudster, they start off with some information that sounds very plausible that they might be calling from the bank or law enforcement. It is an impersonation scam to victims about being from a bank or law enforcement.

I guess that someone who has already been a victim is marked, rather cruelly, by fraudsters as a sucker. They are people who might be susceptible to a reloading scam. In fact, at the moment, my organisation, on behalf of our members, is creating a victims of scams database. We have evidence that someone might have their first account cleaned out, but then the fraudsters might come back if they find out they have a savings account with a building society, for example. We have definitely seen that happen. They will know that someone can be influenced, and might be under the spell of a scammer. We need to share that information, but do it in a way where we protect that individual so that they are not excluded from financial services. It is a delicate balance around sharing information but protecting the individual.

Q95 **Alison Thewliss:** It is a safeguarding concept.

Mike Haley: You have to safeguard them, yes. It is around giving the information to financial institutions and others to cocoon someone who has been a victim. Re-victimisation is a serious issue. It could be an elderly person who cannot go back to work, for example, or won't go back to work because of their age, and their savings have gone. They are the heartbreaking cases.

Sophie Davis: We see cases of people who do not recognise their own victimisation. For example, with romance fraud it can happen that people are so convinced by the relationship that they do not want to believe that the fraudster is a fraudster. They leave themselves open to repeat victimisation and to different types of victimisation. It is called "sextortion", where the fraudster can use any images that they have used of them to extract further money from them. In those cases it is partly around the support that the victim is given, and a more enhanced form of support to try to enable them to get out of the grips of the fraudster.

Q96 **Alison Thewliss:** Thank you; that is really interesting. I want to pick up on another thing that you mentioned, Mike, around people making more false applications or people becoming a bit more scammy. Is that a hangover from covid, when people could apply for things or for additional support? From my own casework I have seen a situation where people ordered goods and said that they had not been delivered, when of course they had been delivered so they were defrauding retail companies in that way. How commonplace is that?

Mike Haley: Over the last three or four years, we have started a longitudinal study over time, surveying ordinary consumers on their attitudes to different fraud types. About four years ago, one in 12 people said they had either done one of the behaviours, such as ordering goods and saying they had not been delivered, or ordering goods, wearing them and sending them back—everyday frauds, if you like—or gilding the lily on their insurance claims or money muling. We found that it went from one in 12 to one in 10 to one in eight. Over time we are seeing that people are more likely to think that some of those behaviours are appropriate or reasonable. The highest ones are on things like online retail fraud, which lots of people said is reasonable. Quite a lot of people think that money muling is a reasonable thing to do. They don't see the harm in it, perhaps.

Why do we think that over time people seem to see fraud as less a crime and more a reasonable type of behaviour? It would be interesting to do a bit more research. You will have to speak to some of our research colleagues. It could partly be driven by economic conditions. It could be around the general tone in society about whether fraud is being decriminalised because you don't see many people's collars felt, particularly for low-level, day-to-day fraud. In the end there should be a repercussion for fraudulent behaviour, for ordinary people as well as the people at the top of the tree.

Q97 **Alison Thewliss:** Is it because, if these things are happening online, it is a bit more faceless? People in the past might have been embarrassed to go into a shop and say, "Oh no, I've not worn this," or, "I've not done this." Now, you can fill in an online form and you never actually see the person you are defrauding?

Mike Haley: Absolutely one of the reasons why we have seen fraud increase is the broadening of those who think it is reasonable. If you had to go into a bank and make a false application for a mortgage and say, "These are my payslips," you would need some bravado to do that. You would have to sit in front of someone and lie to an individual. With intermediation through the internet, there is a faceless bureaucracy. It might be a Government service that was paying out. We saw that with bounce-back loans. There were online applications. You are lying to a machine. You are probably not overthinking that. It is the same with any online accounts that people have. I think that has been one of the drivers of greater fraud. It is seen that you are less likely to be caught. I think

people feel, "We have heard of other people doing it," and, yes, it is faceless.

Richard Hyde: Going back to the point earlier about research gaps in our knowledge, it is to what extent the increase in fraud is driven by criminals switching from what they were doing previously to fraud because it is easier now, and they are less likely to get caught compared to their previous criminal activities. That is a big gap that we do not know the answers to yet. It is an important question. Is it the same pool of bad actors just shifting in response to incentives and shifting their activity, or is it new people coming in and doing it?

Alison Thewliss: Thank you very much.

Q98 **James Daly:** I want to ask a question which is related to the reality of the position. Is this epidemic of fraud too big, in some senses, for us ever to have a complete answer to it? From the nature of what you are talking about, it seems to me that we would have to have an incredible increase in the number of police officers and the various technical skills that go with that. Is it a question of mitigating rather than finding solutions, or am I being too pessimistic?

Mike Haley: It is a really great question, Mr Daly. We have got to a stage where there is an epidemic of fraud and we need to understand the sophistication. It is a broad set of activities, from corporate fraud through to very individual frauds plus the organised crime elements. Among that, even in investment scams, romance scams and purchase scams, understanding the issue in more depth enables more targeted strategies around the different fraud types. We need to have a better understanding.

Am I pessimistic about getting on top of it? No. There has been some investment. We need to look at upping the targeted enforcement action against the highest-harm organised crime and the individuals. We might find from that that quite a lot of fraud and crime is being perpetrated by a small number.

Q99 **James Daly:** That is quite different. If I understand you correctly, it is advising the Government, the police and the National Crime Agency to proactively take steps against identifiable bodies. One of the things that concerns me is law enforcement in terms of the reactive nature to a complaint, which may be a relatively low-value fraud.

The problem that we have is that, even with a relatively low-value fraud, the nature of the evidence that is required for the matter even to get to the Crown Prosecution Service, let alone into court, is vast. Even on non-fraud cases at the moment you are talking months to get the most basic sets of paper evidence, if I put that in the correct form. It is very interesting—I think this is what you are saying—that the way of preventing this is being more proactive rather than reactive.

Mike Haley: I think I should have introduced my earlier points. There needs to be a strategy which covers an increase in law enforcement and more public awareness as part of the whole strategy, as well as industrialising prevention and detection. This is such an industrial style of crime that we need to look at how we share the information and data to be able to stop bad actors getting into the system in the first place. We need to industrialise prevention and detection.

The Home Office fraud strategy, which was long awaited, put prevention through industry at the heart of that. As you say, we are not going to arrest every single fraudster. Even if you did, you would have the issue of whether the courts would be able to cope with it. It takes years. We need a prevention first strategy and a prevention mindset when it comes to fraud.

Sophie Davis: I completely agree with that. There should be increased law enforcement because we do not want to give the impression that it has vacated the pitch and it is a consequences-free crime, but it is not something that we can arrest our way out of, for all the reasons Mike explained. We need a much more proactive approach. As Mike says, that is partly by getting better intelligence and data sharing as to who the lead organised crime gangs are that are driving this, and the patterns, so that we can stop it at source. We have to design it out. We have seen some real success in other crime types over the last few decades, such as car thefts, burglaries and others in terms of designing out crime, which we can try to implement in the same way.

Q100 **James Daly:** Again, I may have misunderstood slightly the prevalence of fraud. My postbag may be different from other colleagues on this Committee. I get lots of letters regarding various criminal matters. Fraud does not tend to be as prevalent. Are we at the stage now where people are shrugging their shoulders, if they are the victim of relatively low-scale fraud, not reporting it to the police and just accepting it: "I've been scammed and I will learn a lesson from this"? Is that where the general feeling is?

Sophie Davis: We carried out a survey of about 3,000 individuals and 700 businesses. We asked them which crime types they were most worried about being affected by. In our survey, with the limitations of a survey, the crime that came up as the one that the public was most worried about being affected by—not worried in general—was online fraud, above other forms of crime. It suggested, at least from the research that we have done, that people are worried about this and that it is something that concerns them. We found the impacts were quite wide-ranging in the emotional and psychological impacts on people. That suggests that people are not necessarily shrugging their shoulders at the idea of being a victim of fraud.

Q101 **James Daly:** I know precisely zero about technology, so you are going to have to treat these questions in that vein. I was sitting in my office the other day and receiving direct messages related to one of my social

media accounts. They were quite clearly fraudulent. They were quite clearly messages which certainly did not appear to have come from individuals. My office hurriedly told me that if I had pressed on that button, if I had opened up the social media message, it would have given potential fraudsters access to lots of information related to me. Is that correct?

Sophie Davis: Yes, I think so, potentially.

Q102 **James Daly:** It is just for my understanding, in the sense of getting hold of personal information and its relationship to social media. How does that work? Is there a piece to be done in respect of that?

Richard Hyde: If you had clicked on that link, for example, it could have been a number of things. It may have put a key logger on your device which would then have reported back to whoever sent you the message what keys you were pressing. If you were typing in passwords and so on, they would know your password. Another option is that it could have taken you to a website and, if you had carried on engaging with that activity, it might have asked you to put in details. That website would not have been a genuine website but one run by the fraudsters. That would be a way of harvesting your details.

Q103 **James Daly:** Is that type of targeting happening throughout the community and throughout the country? It is not because I am an MP that I am getting messages like that. People are targeted in general. That is the definition of an epidemic, isn't it? Thousands, if not millions, of people every day are getting sent things that could potentially open them up to fraudulent activity.

Mike Haley: We absolutely see that. We have all these names for it: phishing, smishing and vishing. They are all attempts by email, texts and phone calls to get some information. They do it at mass scale because most people recognise that it has not come from a genuine source. It is a bit of an arms race because the scammers now will impersonate; they have tools to be able to appear that they are coming from your bank's telephone number. It will look like the number that you are being called by. At the network level, all of this needs technical countermeasures to be able to stop so many of these messages getting to people in the first place. If you can cut that off, you are cutting off the information.

As Richard said, there are a number of things. It could be that you have downloaded some malware on to your device by just clicking. It could be something where they can take up ownership of your device, like a TeamViewer type of thing. Mainly we see it as an online form because it is asking you for the credentials to start getting some information. They are asking you to fill in a form, and that is then stealing your identity or your credentials for account takeover. It is not just because you are an MP, Mr Daly. Every one of us gets those.

James Daly: It is a very good example, though. I am not saying it for public education. Obviously, as you say, the public are very much more

aware of these things these days. It is the very public stance of public bodies—the Government or whoever it may be—in putting these things into the mind of the public that is probably going to have a bigger impact than some of the law enforcement measures that are obviously needed and are necessary in these circumstances. That was very interesting. Thank you very much.

Q104 **Chair:** Mr Haley, could I go back to a comment you made about there not being legislation dealing with holding identity information about an individual? We heard earlier that 70% of frauds emanated from overseas. Do you think that amending the legislation on identity fraud would really help, or is it bigger than that because of the overseas element?

Mike Haley: Together with law enforcement action against those who are collating and selling identity—giving the tools to law enforcement—there would need to be some concerted action around going on to those websites, which are in plain sight, and getting them taken down because they are creating an offence. That could then be said to be hosting of those websites, and you could take them down because it is an offence, rather now, when it would not be. It is a step towards that. It would not be a panacea.

Q105 **Chair:** That's great. Finally, I want to ask each of you this. When we put together our report, what is the one recommendation that you would really like to see in it? Mr Haley, I am sure you have lots.

Mike Haley: I do, but I will choose one. What is lacking at the moment is system leadership and co-ordination. We have so many different agencies who have an interest in fraud, but it is not their priority. I would like to see a Minister for economic crime who can work across all of Government and is empowered by the Prime Minister to co-ordinate that activity.

Q106 **Chair:** That is very clear; thank you. Mr Hyde.

Richard Hyde: That is very important but probably for us, going back to Mr Daly's question, we have suggested an uplift in police and their support workforce of about 30,000, specifically focused on economic crime issues, and within that fraud. That would rebalance policing towards reflecting fraud as the proportion of crime that it is. As we were just saying, it is a very difficult crime to organise. That would give you the number of people to actually have a proper go at tackling the problem, at least on the law enforcement side.

Q107 **Chair:** That is very helpful. Ms Davis.

Sophie Davis: I would probably have said the same as Mike, so I will pick a different one, just to have something else. It would probably be greater incentives on some of the actors in the chain, particularly social media companies and other online firms.

Chair: That is very helpful. Thank you very much for your evidence this morning. We will be producing a report, probably in a few months' time. Your evidence has been very helpful to us, so thank you.

Examination of witnesses

Witnesses: Professor Ryder, Professor Lord and James Babbage.

Q108 **Chair:** Welcome to our second panel on fraud. I am going to ask you to introduce yourselves. Professor Ryder, I understand you need to make a declaration to the Committee.

Professor Ryder: My name is Professor Nic Ryder from the School of Law and Politics at Cardiff University. I am a special adviser for the Home Affairs Select Committee on this investigation.

Professor Lord: My name is Nick Lord. I am a professor of criminology at the University of Manchester. For the last 15 years I have researched areas of economic and financial crime, such as fraud, corruption and bribery.

James Babbage: My name is James Babbage. I work with the National Crime Agency, where I am the director general for threats. I am responsible for the National Economic Crime Centre, the National Cyber Crime Unit, which has some relevance to these discussions, and a range of other threats. I should probably add that the National Crime Agency is a law enforcement investigative agency, but also takes a strong interest in prevention and preparing the public. It is what we call a four P approach to crime. I am very happy to cover some of those issues as well.

Chair: Thank you. From our first panel we heard some really interesting information and it has set the scene for what fraud currently looks like. I am going to move straight to Tim Loughton, but we will probably come back to some of that in the questions that we raise with you through the session.

Q109 **Tim Loughton:** Apologies that I cannot be here right to the end of the session, which is why I'm going first.

Mr Babbage, I think you were sitting in on the earlier part of the session. We have heard that this is a huge and growing problem; 40% of all crimes are down to fraud. It is very multifaceted, from romance fraud through to terrorism. We have just heard that it would probably take 30,000 police officers, or people working for the police, to tackle this as a proportion of the type of crime that now constitutes fraud, which is one hell of an investment.

This is not crime that is combated by bobbies on the beat wandering down streets. It is very different, so it requires a completely different approach. It probably requires an approach of recruiting loads of computer nerds fresh out of university who have a chance of getting one up on the computer nerds who are the fraudsters on the other side. Is that what the NCA is doing?

James Babbage: Yes. The national fraud strategy also brings into play other employers of such people, such as the intelligence services. If I can

step back, in answer to your question, and give an observation on the changing nature of fraud and the scale of fraud, I thought the earlier session was excellent and I agreed with very much of what was said.

It is important for the Committee to know that the crime survey for England and Wales, which is probably the best single data source because it avoids all the under-reporting that is necessarily in some of the other data sources, shows a statistically significant decrease in its most recent numbers. It is 13% down. It is still a lot and, in fact, all the various data sources, from CIFAS to UK Finance, from reported crime to Action Fraud, are also reducing, but there are various reasons why recorded crime is nevertheless increasing. I can get into that, if you like.

My perspective would be that fraud is very much a growing global risk. The reason, principally, why it is a growing global risk, as we have been hearing, but to bring it out really clearly, is that it is an online crime. People in the UK are potentially open to be defrauded or made a victim by people throughout the world, or using services and facilities based throughout the world. The criminals are only interested in monetising vulnerability. There are so many different types of crime going on. We conveniently lump them together under the word "fraud", but they are still very different.

I shouldn't go on too much. I mostly want to say how much I welcome the inquiry. Your very first oral witnesses got some very good media out about a month later on romance fraud. They are getting the message out to people so that they can understand the sorts of threats. To use that as an example, that type of romance fraud is where the scammer or the fraudster is trying to get you to give them money. There is a set of things that you need to think about and do to be wise to that. We saw someone in Taunton sentenced just yesterday for a very similar sort of romance fraud.

A linked fraud, which is another of the four high-harm frauds that I hope to have the opportunity to talk about in a related question, is romance investment fraud. In that case the fraudster, who is apparently having some sort of romantic connection with you, will be trying to seed things into the conversation to cause you to think that you might invest your money for your own gain, profit and income. Of course, there is a completely different set of defence mechanisms that you have to have ready when you are engaging with that. The fundamental point is that our understanding of trust online is so immature. Because of the reasons of shame and stigma that we have been talking about, and a range of other factors, we are not talking enough or in enough depth and granularity about the sorts of risks that are out there. The pillar of the fraud strategy that is about empowering the public is particularly critical.

Q110 **Tim Loughton:** Going back to my nerd point, we have visited the NCA before, particularly around child sexual exploitation, where you have some really smart work going on with police officers impersonating

potential victims of child sexual abuse, right down to the potential abuser turning up expecting to meet a 12-year-old child but it is somebody from the NCA or whatever.

That seems to me the sort of thing that is going to gather information and implicate some of the fraudsters. I know it is an international problem. We have heard that 70% is based overseas, but even if it is just the 30% based in the UK, entrapment by playing their own game is surely one way of doing it. I did my own little bit when I almost fell foul of the latest text message, supposedly from one of my children who has dropped his phone down the loo and needs to pay a bill urgently. It was really quite smart. Fortunately, I rumbled it and I got their bank account details, rather than me giving them my bank details, which I then passed on to the police. I was quite pleased with myself.

That is how it is going to be tackled, isn't it? There needs to be a risk that the perpetrators are going to be entrapped. At the moment, with less than 1% of reported fraud leading to convictions, they are mostly getting away with it with impunity.

James Babbage: We are cautious about the word "entrapment". If I can take your question as, "What are the nerds doing?", one of the things they are certainly doing is engaging the fraudsters and, on that basis, working out how to disrupt them. In the NCA alone, we increased our number of disruptions last year by 38%. That includes a whole range of things, some of them quite minor. If you look across the whole system of policing, the number of disruptions was up by 15%. That is a larger total, including NCA and others. We think that is about 240,000 frauds avoided.

Something that a different set of excellent nerds are doing now in the National Cyber Security Centre—so much of this is connected to online risk, as a number of you have been saying—is the active cyber defence work, which is well worth looking up. That is taking down fraudulent websites. There are a number of data sources for that, including the suspicious email reporting service. If you receive a suspicious email, you can forward it to report@phishing.gov.uk. That is a company that NCSC works with. They know how to get the sites taken down by the suspicious reporting service. This happens on average within six hours. More broadly, 2.7 million sites were taken down in 2023, which included extortion mail servers and cryptocurrency investment scams. It all feeds into a thing called share and defend, which the CSPs, the service providers, do for all of us. Where the CSPs know that sites are fraudulent, they can block us, their customers, accessing them.

Finally, in a similar spirit, SpamShield is something that the telcos introduced a couple of years ago to try to reduce the volume of fraudulent SMSs—smishing, as it is called. BT says that it resulted in a 90% reduction in malicious texts reaching the public. Certainly the number of reports going to 7726—the number where you can send any of them—was down by 50%.

Q111 **Tim Loughton:** I appreciate all of that. The trouble is that, despite all of that, the conviction rate is still 1% and there were the 3 million offences, just the reported ones last year. Turning to our professors, where in the world does this better than us?

Professor Lord: That is a very good question.

Q112 **Tim Loughton:** Thank you very much. What is the answer?

Professor Lord: First of all, I would like to echo some of the points that James made about what the scope of fraud actually incorporates. Fraud is a very diverse construct. It incorporates behaviours from, on the one hand, things like the pig butchering investment scams that we currently see through to very serious corporate frauds and food fraud, which I look at partly in my own research.

The implications of that diversity are that there are very distinct differences in the individuals who get involved in the different fraud types. They also have different motivations. They have a different modus operandi. They carry out or use different methods to accomplish their criminal goals and objectives. They make use of different networks. If you are a fraudster in an otherwise legitimate organisation or corporation, you may have a ready-made network within that organisation already, whereas an external fraudster or criminal may have to recruit others to accomplish their behaviours. We also see differentiation in the distribution and concentration of victims of different fraud types. We know more currently about volume fraud and much less about serious elite fraud by organisations and professionals.

The main issue, which is important for how we design prevention and intervention mechanisms, is that we currently have very incomplete and inconsistent data about the extent and prevalence of all fraud that takes place in our country. What I mean by that is this. There were some estimates by the National Crime Agency that around 86% of all fraud actually goes unreported. In other words, we are currently basing our analysis and our assessment on around 14% of known cases. The implication of that is that given this large, dark figure of crime, as we call it in criminology and academia, we cannot say too much about the prevalence or the nature of fraud types because there is such a large amount that we simply do not know about.

Of course, the knock-on effect of that is how we design intervention or prevention mechanisms that can deal with a broader range of frauds when we simply do not fully understand the full extent of the problem. I am sure Nic would agree, and that is one reason why we need much more data and research into understanding the prevalence, extent and nature and organisation of a diverse array of fraud types. Once we better understand how different frauds are organised, we can then design intervention mechanisms that can deal with those specific frauds and, in turn, look to see whether or not specific mechanisms can be used for a wider array of frauds as well.

Q113 **Tim Loughton:** I appreciate all of that. What is the answer to my question of who is doing it better? You have told us what we need to do. I think we all agree with that. Who is ahead of us in the game?

Professor Lord: We are doing a very good job actually in terms of how the UK Government are going about dealing with fraud. The fraud strategy, for instance, has a lot of good ideas, such as the creation of a fraud squad, although that raises questions about what the scope of that fraud squad should be, given the diversity that exists around different fraud types. There are things like engaging with big tech companies. That is incredibly important. The online fraud charter is a good example of that, and having corporations sign up to that. That also raises questions around what the fallback plan might be when corporations, the big tech companies, do not engage, collaborate or co-operate with the authorities or each other, and therefore do not do as much as they need to. Prevention costs money, of course, for corporations.

Q114 **Tim Loughton:** Professor, are you telling me that the UK, with a 1% conviction rate, which you say is based on only 14% of actual fraud that is reported, are world leaders?

Professor Lord: What I would say is that I do not think the evidence is there to make an assessment about who is dealing with this best.

Q115 **Tim Loughton:** But you cannot point to another country in the world, notwithstanding the incompleteness of their figures, that has a conviction rate on fraud-related crime of higher than 1%.

Professor Lord: I don't know the data. There may be other countries which have a higher prosecution rate or there may not be. I am not entirely sure. What I would say is that prosecution is not the only potential solution to fraud problems.

Q116 **Tim Loughton:** I understand that.

Professor Lord: There may be other countries doing other things. We use a range of extra-legal mechanisms like education and awareness.

Q117 **Tim Loughton:** I understand that. Prevention is obviously the key. We have heard from Mr Babbage as well on what is going on, but still 3 million crimes were recorded and very few of them ended up with somebody behind bars as a result. Professor Ryder, do you have any more data on the international front?

Professor Ryder: It is difficult to give a direct comparison. If you look at the usual comparison with the US in the academic literature, of course people refer to the FBI and the US Department of Justice. To give you two examples, going back to the global financial crisis of 2007-08, the FBI obtained over 1,100 convictions for mortgage fraud related to the global financial crisis. That was partly fuelled by additional funding provided by President Barak Obama in the Fraud Enforcement and Recovery Act, which is the only law in the world to recognise that financial crime was a key part of the global financial crisis.

Q118 **Tim Loughton:** By mortgage fraud, are we referring mostly to individuals fudging their figures in applying for their own personal mortgages?

Professor Ryder: It was also those working in the financial services sector.

Q119 **Tim Loughton:** To facilitate an individual doing that.

Professor Ryder: Yes.

Q120 **Tim Loughton:** That is not big, organised crime. It is a crime, but it is not the sort of big, organised crime networks that we are most concerned with. It is individuals pulling a fast one in a criminal way.

Professor Ryder: That's true, yes; but what it shows is that if you provide the finances, in this particular instance you end up with 1,100 convictions. If you go back to the savings and loan crisis of the 1980s, you have a very rare example of over 1,000 senior execs of companies being prosecuted and convicted for fraud.

Q121 **Tim Loughton:** They are low-hanging fruit, largely. Somebody trying to fake their mortgage application and pull a fast one over a financial institution is probably pretty amateur. They are not doing it for all their mates and neighbours. They are doing it for themselves. It is still a crime. The Committee is much more concerned about where the big growth has come from organised criminals who have semi-professional outfits and networks going on that are taking advantage of monetising vulnerability, as I think Mr Babbage put it, on a vast scale. It is great that we have locked up 1,100 people in the States who tried to scam their mortgage, but that is not really the heart of the problem that we are addressing, is it?

Professor Ryder: No. I think the low-hanging fruit are easier to investigate and prosecute.

Q122 **Tim Loughton:** To pick.

Professor Ryder: One of the big issues is where you go for senior managers. Obviously, we have seen with the recent legislation in the Economic Crime and Corporate Transparency Act an attempt by the Government to introduce a new senior managers test. Part of the difficulty is that if you look at the basis for that test in the Corporate Manslaughter and Corporate Homicide Act 2007, and the FCA senior management certificate regime, the enforcement of both the corporate manslaughter Act and the enforcement against senior members of regulated authorities is very sparse. There are questions that need to be carefully considered regarding the welcome senior management test.

Q123 **Tim Loughton:** Mr Babbage, do you want to come back?

James Babbage: May I briefly offer some thoughts, both on international comparators and on conviction rates? First, on international comparators, as colleagues said, the UK has been on the bleeding edge of

this problem and is beginning to get its act together earlier than some others. Ms Davis gave most of the reasons for that: English language, faster payments and a more online retail economy. It is 27% in the UK, which is more than anywhere else in the EU or the US by quite some distance. Surprising as it may be in some ways to all of us, and there is certainly good practice in particular places—we have been working with the Singaporeans, for example—I do not think it is the case that the UK is really lagging in this area. We have had the problem earlier.

On prosecutions, there is a range of different factors playing into that. It is the case that both HMRC and DWP are prosecuting many fewer people than they used to. I think both, for different reasons, are focusing on smaller numbers of higher-value criminals. That is ultimately a choice for them.

We need to do more to get more prosecutions, but we need to bear in mind that much of this fraud—77% in our view—has an overseas element. Where you have, both in west Africa and in south-east Asia, camps of 10,000-plus victims who have been trafficked and are being forced basically to run fraud boiler rooms focusing on fraud elsewhere in the world, that is not going to translate, with the best will in the world, into large-scale prosecutions. We are working particularly in west Africa, which more directly affects the UK, with the countries involved. I wanted to add that to what has already been said.

Q124 **Tim Loughton:** Finally, I want to come back to the terrorism aspect of this, which is perhaps more worrying. What is your take on the most worrying aspect to the NCA of how fraud is being used to fund terrorist operations?

James Babbage: The investigative lead for terrorism is in the Met Police, NCT policing. Broadly speaking, the economic crime system seeks to support that as best we can to ensure that we discover, manage and prosecute terrorism. The suspicious activity reporting regime is a key aspect. We have both the defence against terrorism finance, SARs and then the regular SARs. There were roughly 1,000 over the last three years cumulatively on defence against terrorist finance. There are a little over 3,000 suspicious activity reports. There is a dedicated area within the UK financial intelligence unit, which sits within the NECC, which works with the national terrorism financial intelligence unit within the Met. That all feeds into their radar picture of what is going on and how they can find terrorists.

It is true, as Professor Ryder's written submission draws out, that, in particular cases when investigations look back over whether opportunities were missed to use knowledge of fraudulent behaviour, some of that has been found. My impression is that the terrorism system is quite creative in using the full range of legal levers at its disposal to manage terrorism once it has discovered it.

Q125 **Tim Loughton:** Mr Ryder, I think you have a particular interest.

Professor Ryder: Yes. I thank Mr Babbage for that really important point. The difficulty with fraud and terrorism financing is that it is very much an under-researched topic. I have spent about four and a half to five years looking at it in painstaking detail. Sadly, what I have concluded is that terrorists have a black book, or dossier of online documents that I've not seen, because I might be breaching the Terrorism Act by looking at them directly, but I have secondary sources. Terrorists log online and get an A-to-Z guide of frauds to be committed. What the research has indicated is that things like passport fraud and immigration fraud are more relevant for international terrorists. What is a particular threat, of course, is financial fraud, debit card fraud, credit card fraud and identity theft.

If you look at some examples of how terrorist attacks are financed, fraud is a significant proportion. Up until last year fraud was not regarded as a national security threat by the UK Government. Now, of course, it is. Fraud is one of the principal reasons in how the IRA were financed. For decades it is as if there has been a disconnection between the fraud strategy and the terrorism financing strategy. If you break down, for example, the terrorist attacks on 7 July 2005 in terms of publicly available information, fraud is a key aspect.

If you move on to the Manchester Arena bombing and Salman Abedi, there is a link into possible fraud of the Student Loans Company in terms of the student fees and the loan that Abedi was given. To make matters even worse with the higher education sector, we have just done a new study that has concluded that universities are not bound by the anti-money laundering or the counter-terrorism financial reporting obligations. Luckily, cases in those areas are very rare but, as Mr Babbage indicated, terrorists are very adept at evolving their funding mechanisms. I could talk for hours and give you list upon list of how terrorists are financing. What we have concluded is that fraud has become a funding mechanism of choice. It can result in terrorists buying low-capability weapons and, sadly, committing acts of terrorism.

Q126 **Tim Loughton:** I was in Iraq recently, involved in an archaeological excavation. I gather that, during Daesh's reign there, antiquities trading and fraudulently claiming their provenance and things like that was the second largest income after drugs in many of those regimes. It was very organised. You had to have a licence from Daesh in order to rob archaeological sites. You could not just go round willy-nilly. I think 80% of your finds and proceedings went to Daesh, and you got to keep the 20%. It was quite organised grave robbing.

Professor Ryder: It is. I did some research on Isis's funding models in 2018. What I concluded is that they have a corporate funding model, based on how a company operates. That Daesh funding model is based on how the IRA operated for decades. They would have a chief financial reporting officer and a CEO. They would pay terrorists a weekly wage. They would compensate family members of suicide bombers. They even

had their own currency. We had never seen that before. According to American literature, Daesh actually learned from the mistakes of al-Qaeda and other terrorist groups. It has taken terrorism financing from what might be the non-profit sector or private donors to an nth level that we have never seen before in relation to that particular funding model.

Q127 **Chair:** Does the Government strategy on fraud have anything in it to address the link with fraud and terrorism?

Professor Ryder: To echo what Professor Lord and Mr Babbage said earlier, the fraud strategy is to be welcomed. There are several interesting and important developments. Sadly, though, the fraud strategy mentions terrorism on only four occasions; that's it. It does not give any policy guidelines or recommendations as to how to tackle the link between fraud and terrorism financing. What our research has concluded is that that is a possible weakness in the UK Government's strategy. Previous national risk assessment reports published by HM Treasury have all indicated that there are loopholes in the link between terrorism and fraud, but from my understanding the loopholes have not been closed. Again, I think that is a loophole that terrorists will continue to exploit.

Q128 **James Daly:** Professor Lord, I think I understood that you said we don't know the level of fraud in this country or the nature of fraud in this country. Clearly, when you are looking at a strategy to tackle something, a certain amount of knowledge of what you are trying to tackle is helpful. In terms of how we address that problem, I am assuming it is through people like you. Do the Government have a part to play? How are we going to tackle the lack of knowledge?

Professor Lord: There are a number of things that we can do. First of all, we need more research in using different methodologies to help us understand that large, dark figure of fraud. That is the use of things like victimisation surveys and studies, self-report studies and innovation in detection and intelligence to help us close the size of the dark figure as it currently stands.

What we can do as well is gain a better understanding of what we know about particular frauds and how they are organised. We can draw on case file data from the law enforcement authorities and the regulators, although I would add that it is very difficult for academics to gain access and insight into those data. Other countries do that much better. For instance, the Netherlands has mechanisms in place for the sharing of data with academics on cases of organised crime and financial crime. They collate a joint dataset, so academics can easily interpret and theorise about the nature of organised crimes in the Netherlands. It is much more difficult to do that in the UK. None the less, we can collaborate with enforcement authorities. We can look at known cases that come to our attention through investigative journalism as well. There are a lot of good pieces of work.

Q129 **James Daly:** One of the problems from a politician's perspective, when you are considering what level of investment is needed to tackle a problem, is that, if we do not know what the problem is, it is a bit difficult to make an educated guess about how much money we should invest in it to tackle it. Do you think that is an outrageous thought or is there some truth in it?

Professor Lord: There is some truth in that. We know that fraud is a major problem, based on what we know about fraud. It represents 40% of all crime. As things currently stand therefore, in itself, from what we know, it is major. We recognise that, based on the NCA's estimate of 86% as the dark figure of fraud, we can presume that it is much greater. Therefore, anything that we invest in dealing with the problem as we currently understand it will not necessarily address that larger proportion.

Q130 **James Daly:** I am assuming, in terms of what we know, that if you take an amount of fraud-related criminal reports over a period of time, they can be broken down into categories, whether it is terrorism at the more serious end, banking fraud or anything else. I am assuming that we have those figures. Do we have those figures?

James Babbage: May I come in, Mr Daly? The first thing is that I can offer a comparative perspective on the maturity of our understanding across different crime types. We are putting together the national strategic assessment of serious crime at the moment, as we do every year in the UK. It is a fair comment that the fraud input to that is somewhat more immature than some of the other areas. I would probably draw out firearms as the most mature, which is unsurprising. The reasons for that are partly that we have been going after firearms really seriously for so much longer, whereas fraud is something that we are going after really seriously now, but that has been for three and four years and not for a long time. The second reason is that the fraudsters are changing their tactics more quickly because of the online and other dimensions.

We need to be a little bit careful with the dark fraud thing. The crime survey for England and Wales figure—the 2.9 million adult victims and 3.3 million incidents—is not particularly prone to under-reporting. The crime survey for England and Wales rings people up in a statistically methodological way to ask, "What has happened to you over the last year?" Whereas, yes, the recorded crime figures are subject to under-reporting, the crime survey for England and Wales figures are not, subject to any comment that Professor Lord has on that.

Professor Lord: The crime survey for England and Wales does not capture the full extent of fraud types. It is very narrow in its interpretation. Would it ask people about their victimisation in corporate frauds, for instance, or their victimisation in terms of food fraud? Most likely, not. There is a very specific definition of what fraud is in the survey. We need more victimisation surveys to help us understand victimisation across a broader range of fraud types.

James Babbage: It is principally about fraud against the individual. As to fraud against companies, the Home Office did an economic crime survey in 2020 and are running another one in the coming months. There is very interesting data on fraud against companies, actually. Of course, the Public Sector Fraud Authority leads on fraud against the state.

Q131 **James Daly:** I want to ask a question about the nature of evidence gathering in your organisation or the police. A lot of these offences are committed outside the United Kingdom. I imagine the difficulties in getting hard evidence that can support a case are extreme; I do not know. Can you give us a flavour of the time involved in finding that evidence and going to the various agencies that you have to do?

James Babbage: You are absolutely right. This is partly why relying on victim reporting and a reactive approach has its limitations. I have seen figures that only a third of victims have any contact with the fraudsters, and only a sixth can say anything useful about the person they have interacted with. I indicated that disruptions are up. The reason for that is that we are taking a much more proactive approach, as you were talking about in the earlier session, in its being intelligence-led, from intelligence agencies and from our own sources and international partners. We are looking to disrupt frauds as crime in action.

If you can actually burst into a boiler-room where fraud is going on and seize material, you are much more likely to be able to disrupt the fraud, and perhaps prosecute it. There was a good example in eastern Europe a couple of years ago, in September 2022. We knew that an OCG was running a recovery fraud—you talked about this earlier; a post-investment fraud—under the guise of being the Financial Conduct Authority. We were able to work very rapidly with the Romanian authorities. The digital materials seized showed that there were over 50,000 UK targets out of hundreds of thousands globally in their minds. We could already see, from what we seized when we did the disruption, that the UK was seen as an increasingly hard target. We believe we nipped that activity in the bud, in that we got into it before the majority of the fraudulent attempts had taken place.

There have been all sorts of other good examples. The north-east regional organised crime unit with Durham constabulary and Northumbria police disrupted some courier fraud last year. Courier fraud is the exception to the online rule, because the courier bit is someone coming to your door and either taking your cards from you under the guise of being your bank or the police, or even escorting you to the bank. It is just awful. With courier fraud, you are interested in the overlapping nature of fraud, and it very much hooks into organised drugs and firearms crime groups within the UK. Again, both in the north-east, as I was saying, and in a much earlier operation in West Mercia, the whole system, and policing too, have had some good successes disrupting fraud in action.

Q132 **James Daly:** Professor Ryder, I have a final question that touches on all

the subjects. We produce reports and, hopefully, because we have recommendations at the end of them, we don't want the recommendations to be wishful thinking. What I am struggling with in respect of what we are hearing, which is worrying, interesting and educational, is that it is such a big problem that there is no solution that this Committee can specifically put forward. I do not think there is an amount of money or police officers that we could say would definitively achieve it. There may be a few more people who face prosecution because we have more people to do the work in respect of it, but it seems to me that we do not understand the problem. I would like your comments in respect of that.

Secondly, dealing with terrorism and people trafficking is a very different matter from lots of other fraud. In terms of public education and the action that the public can take themselves, how big a part does that play in the country's fraud strategy?

Professor Ryder: Thank you for the questions. Public awareness is essential. If you look back at previous examples—at what was the Financial Services Authority before it became the FCA—they had a public awareness statutory objective of raising consumers' awareness of what could be a possible scam or investment. Based upon published work, a public awareness scheme is essential to raise awareness. There are some very good examples in the financial services sector regarding bank consumers. We know that obviously the NCA regularly publishes SARs updates online on increased awareness for potential victims of fraud.

I don't think you can make recommendations to tackle everything about fraud. You are right. There is such a huge issue in relation to the extent of fraud, as we have argued, and the number of cases that are reported and the fraud that is not reported. There are some very basic recommendations that could improve, for example, data sharing. They could improve the exchange of information between the public and private sector and in the public sector. Professor Lord mentioned the Netherlands example and how that is regarded by the Financial Action Task Force as an example of best practice.

I have just finished some research with a colleague, Dr Samantha Bourton from the University of the West of England Bristol, and we have challenged the Financial Action Task Force conclusions on the UK's own exchange of information mechanisms. From a fraud and terrorism financing perspective, we found some anomalies in the legal framework that we think could simply be amended by reform to pieces of primary legislation that could close a loophole in that area. I think you can start small. That might help to solve some of the loopholes.

Q133 **James Daly:** My background is in criminal law. I am still going to come back to that challenge. I don't know how you address the fundamental difficulties in the job of addressing fraud. The challenges are so vast. If a basic fraud happened in a police force—it does not matter which police force it is in the country—that involved the downloading of social media

records and bank accounts, the amount of time that the most basic fraud would take for the police to investigate, and I am not criticising them, would be months at this moment in time.

James Babbage: The first point, I think, is that fraud investigation is not impossible. There is a people strategy in this area being run by the City of London police. The recruitment of more people for the fraud squad means that we have people who are able to do this. We should avoid giving the impression that it is not something that can be done by regular investigators, because to some degree it can.

We talked about the role of technology and technology companies a little bit in the earlier part of the session but not very much, and possibly not enough. If over 80% of this is online, we have to focus on what more the technology companies can do. In general, there is heaps more they can do. If you receive an email and it is from a very newly created domain, that is a red flag that your email provider could in theory show you alongside the email. If you receive an email from an address that is very similar to one that you correspond with a lot, but just slightly different—a 1 for an L or something—that is something that the technology ought to be able to flag to you. Similarly, if you are on a social media application and the person you are talking to has various indications of inauthentic behaviour—let's say that they appear to the tech company, to the platform, to be somewhere other than where their profile says they are located, or they appear to have hundreds of different accounts or even possibly to be messaging unusually large numbers of people. It is finding ways to make more transparent the stuff that the platforms understand and that as consumers either we do not or it is too complicated to check.

I want to say again that I think we are doing some of the right things in the UK. In particular, the mix of the Online Safety Act—compulsion—and the online fraud charter, a voluntary mechanism, are world leading. There are some similar activities. The eSafety Commissioner in Australia is worth a look. They are world leading. In particular, the online fraud charter—the voluntary one—has a requirement on marketplaces to introduce "Know your customer" style verification for sellers. If that is fully implemented in the next six months, as the 11 signatories have signed up to, it could make an enormous dent in the volume of fraud. I hope that helps.

James Daly: It does. Thank you.

Q134 **Chair:** But only if they do that.

James Babbage: Of course.

Q135 **Chair:** Why are all these platforms not selling themselves: "We're doing all this really super stuff to make sure you're safe" to attract more people to their platforms? Surely, it would be a selling point that they are going to tell you if something is a bit dodgy.

James Babbage: That is a really fair point. You should ask them that. They have, however, signed up to doing this within the next six months, so I am positive in my feelings about what we are leading in the UK and the potential for them to make a difference. It is surprising that online safety is not more of a differentiation in terms of buyers on platforms. We do not know, just round the table, which one is safer than another one.

Q136 **Chair:** Professor Lord, you want to come in.

Professor Lord: I entirely agree that the scope and the scale of fraud is very difficult, which makes it very difficult for the enforcement authorities to prevent. One plausible way to reduce the harms associated with fraud is through what we call situation prevention in criminological terms. That requires a much more detailed and comprehensive understanding of what we call the opportunity structures for certain kinds of criminal behaviour like fraud. What are the features or conditions of particular fraud types and how do they need to come together to enable a fraudster to carry out that behaviour?

Once we understand what the opportunity for a different kind of fraud looks like, and we can do that comprehensively across all fraud types, we can build what we call scripts. We can break down the crime commission process, or the fraud commission process, into its constituent parts and stages to understand what stages criminals have to go through from start to finish to accomplish or carry out their criminal objectives. Once we have a comprehensive understanding of the nature of the criminal behaviour, we can design interventions at different stages of that criminal process. If it is at the point of intersection between individuals and their online social media platforms, we can design methods or mechanisms that make it much more difficult for criminals to carry out fraud via that particular platform or pathway.

By understanding comprehensively the nature of criminal behaviour and who gets involved in these crimes over time and at different stages of the criminal process, we can look to models of situational crime prevention that encourage us to identify how we might increase the effort for offenders to carry out their behaviours; how we might increase the risks of offenders being caught through different forms of detection and intervention; how we can reduce the likely rewards for offenders or remove the provocations that might be incentivising or motivating them to carry out their frauds; and how we can remove the excuses they might use to justify their fraudulent behaviour. In order to carry out that kind of comprehensive analysis into all fraud types, we need much better access to the data to allow us, as academics, to gain insight into how criminals go about organising their behaviours.

Q137 **Alison Thewliss:** I want to start by picking up some points from the earlier part of the session around data sharing, and how we go about tackling the situation. Mr Babbage, what difference will the Economic Crime and Transparency Act make to data sharing?

Q138 ***James Babbage:*** I cannot answer that as a specific question. I can answer about data sharing more generally, if that is helpful. Sorry about that.

The first thing is that I very much agree that a more structured and comprehensive approach to data sharing is an important and very significant difference we can make. It is in the fraud strategy and the Home Office are working on it. We are working on it with them. Broadly speaking, there are law enforcements aspects of that, there are industry aspects, and then there are other aspects, such as with academia. I will take away Professor Lord's very helpful thought on that.

I want to share that we have had the joint money laundering intelligence team—the JMLIT—which Professor Ryder referred to, since 2015. It now has 46 partners. It focuses more on money laundering but, as we have heard, that is very relevant to fraud. Over time, it has allowed us to make over 300 arrests. We have almost £200 million under restraint. A couple of years ago we launched JMLIT Plus, which allows us to involve some of the other sectors that Professor Ryder referred to in his written material. That allows us to get a collective threats picture and an agile time-banded approach with particular cells.

We did a pilot, maybe 18 months ago, with two banks to share a lot more data than we normally share. I am not in a position to make further announcements on taking that forward, other than to say that we are in very active discussion about taking it forward. I hope, possibly before the Committee concludes this inquiry, that we will have more to say about how we are looking to proactively share data in a public/private way with a much larger group and, in part, particularly going after fraud.

Q139 **Alison Thewliss:** That is interesting; thank you. I look forward to hearing more about that later on. Having previously had a Treasury spokesperson role, I am quite interested in the way in which UK corporate structures can facilitate a lot of this fraud. Lots of people were registering obviously fake companies at Companies House, which had no real process to interrogate that. They were only a library rather than an interrogation organisation for the information that they gathered. Has there been much communication between the NCA and Companies House, given the new powers that they will have both to interrogate new companies coming on to the register and existing companies on the register that have clearly been used for fraudulent purposes?

James Babbage: Yes, there has. Companies House reform is something that we have argued for within government. We are really pleased to see the new provisions there. We think they will make a real difference. We are hoping to increase our liaison with Companies House as well. You are absolutely right to say that it is very important to deal with that issue.

Q140 **Alison Thewliss:** Based on the Companies House register, there are hundreds and indeed thousands of companies based at a single mailbox address. From your perspective, is much done to interrogate those

companies? To me, it would seem a very obvious flag of something suspicious, but I am not clear as to how much that gets followed up by people with responsibility for interrogating frauds. Those companies are clearly not what they purport to be. They often register false names that sound like a company, for example.

James Babbage: There can be legitimate business practices that involve the registration of multiple companies at a single address, but I agree with you that anything that gives us more data and the ability to share that data and pull it together with other forms of data is to be welcomed in proactively getting after these risks.

Q141 **Alison Thewliss:** I would be very keen to see more happening on that. Related to that, there have been previous investigations by, I think, "File on Four" looking at the recruitment of people on social media platforms to serve as company directors. They are not actual company directors. They are not fulfilling any duties of company directors, but they are named on the company paperwork. That is among a number of ways that criminals and fraudsters use social media to recruit people, perhaps in private groups that organisations like yours might not get to see. What conversations do you have with social media companies about how those groups operate within their systems?

James Babbage: Broadly speaking, social media companies increasingly put the contents of such groups beyond their own ability to see and moderate. Secondly, even where the social media companies can see them, they take quite a firm view of what the boundary of illegality is. It is possible that some of the behaviour as seen in individual groups would not be seen by companies as illegal, even if becoming a company director might be an offence. It is a very difficult and grey area that is, again, worth following up on with social media companies, particularly those that are getting out of the content moderation business.

Q142 **Alison Thewliss:** Should there be more focus on that by Government? It feels as though the social media companies get away with a lot in those terms. I remember conversations about this over the years when the Treasury Select Committee looked at economic crime and what social media companies actually do about what is being facilitated on their platforms.

James Babbage: As I mentioned a few minutes ago, the Online Safety Act is world leading, although there are some other countries in a not dissimilar place, and sets the basic terms of trade about right, in putting an onus on the platforms to look out for online safety and a serious financial penalty for them if they do not.

The whole situation will continue to evolve very fast. Ofcom has a consultation out now on the regulations. We need to see how those regulations play out in practice. I am sure that over time they will not be able to stay static. It is something that we are all going to have to keep very much on top of.

Q143 **Alison Thewliss:** It seems to me that everything from money muling, investment fraud and all kinds of scams and selling goods which do not exist flow through these companies. It does not matter which platform it is.

James Babbage: That is absolutely right. As a rule of thumb, the bigger the platform, the more of it there will be.

Q144 **Alison Thewliss:** Do the professors have anything further to add on the way in which crime is facilitated through the structures that we have, and what more can be done around that?

Professor Lord: The misuse of corporate vehicles or companies as part of the organisation of serious crimes for gain is an area on which I have done a bit of research as well. Again, I point to the Netherlands where we saw a good example of the creation of a screening authority. It was there to screen any corporations that had engagement with public sector procurement contracts; to scrutinise the companies that had been formed for the particular purpose of tendering for public contracts.

Clearly, the issue is very broad and large and difficult to deal with. It is very straightforward for criminals to circumvent some of the mechanisms put in place by Companies House, and what will be put in place. A good starting point is for us to look at public procurement issues in particular and see whether or not we might give Companies House, or some other authority, the capacity to deal with scrutinising companies that are created for that sole purpose.

Q145 **Alison Thewliss:** Obviously, a lot of that was through covid.

Professor Lord: Covid being a good example of that.

Q146 **Alison Thewliss:** Absolutely. In the NCA's engagement with Police Scotland and the Crime Campus at Gartcosh and the Serious Organised Crime Taskforce, what is the relationship like there?

James Babbage: It is generally a very positive relationship. What I want to add to the earlier conversation on fraud in Scotland was that the Scottish crime and justice survey takes a slightly different methodological approach from the crime survey for England and Wales. It focuses on cyber-enabled fraud. That generates even higher returns of people saying that they have been affected. If we are trying to work out why that might be—I am now speculating—I think it is because of the wider variety of account takeover type behaviours that were mentioned in the earlier session, and which certainly feed into the broader fraud landscape. Crest Advisory has done a similar survey in England and Wales, which generates similar levels.

My feeling is that the prevalence of fraud in Scotland is likely to be broadly similar to the rest of the country. Equally, the 77% that is overseas-based or partly overseas-based is likely to seek to victimise people in Scotland as much as people anywhere else. The intelligence-led

activities that we are taking forward to counter all of those, and the prevention activities I have referred to earlier, should help right across the board.

Alison Thewliss: The figures that I found were broadly in thirds; 31% were suspected and confirmed in Scotland; 32% were suspected and confirmed outwith Scotland; and you could not establish where the criminals were in the remaining 37%. That is part of the issue when there is so much you can do to disguise your location. You just cannot find out where these people are at all, which is quite concerning.

Q147 **Chair:** Can I ask each of you for a key recommendation for the report that we are about to write? Professor Ryder, you may already have given us quite a few recommendations.

Professor Ryder: Ideally, as was said in the earlier part of the session, there needs to be an economic crime Minister, and there needs to be a single Government Department that manages financial crime, because each Government Department has a particular strategy and agenda, whether it is DWP, the NHS or the Home Office. There needs to be a single Minister with a portfolio and a Government Department that purely looks at financial crime.

Q148 **Chair:** That's good. Thank you.

Professor Lord: I suggest two things. First, quite selfishly, we need more or better data sharing with academia, so greater access to data in order to generate—

James Daly: Like the University of Manchester.

Professor Lord: The Universities of Manchester and Cardiff would be good.

Professor Ryder: Get the plug in.

Professor Lord: More can be done on developing mechanisms for a data- sharing approach between academia and law enforcement authorities and regulators. Secondly, to help us to understand what actually works to reduce harms associated with fraud and other related types of crime, we need much better before and after data on particular intervention mechanisms, to understand what works and under which conditions, in order to develop a more systematic and robust evidence base to help us understand, "Well, this works in this instance; therefore, we can use that." We do not currently have that.

Chair: Thank you for that.

James Babbage: For me, it is principally about staying the course. Bearing in mind that the nature of fraud will continue to evolve, we need to keep an eye on that. The economic crime plan 2 and the fraud strategy have a whole range of actions, particularly with the Online Safety Act. It is just being persistent about carrying those through, testing out what is

working better and what isn't and keeping up the existing plans for growth of resource in this area.

Chair: Thank you very much for your evidence today. It has been very helpful. As I said earlier, we will be writing a report. The recommendations that you have put to the Committee are going to be very helpful in our discussions, so thank you very much for that. If there is further information you want to share with us, please feel free to do so. I am particularly looking at you, Mr Babbage. If your conversations develop into something, it would be helpful to know about that. Thank you again.