HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Fraud, HC 125

Wednesday 28 February 2024

Ordered by the House of Commons to be published on 28 February 2024

Watch the meeting

Members present: Dame Diana Johnson (Chair); Carolyn Harris; Kim Johnson; Tim Loughton; Alison Thewliss.

Questions 296 - 397

Witnesses

I: Assistant Commissioner Nik Adams, City of London Police, James Babbage, Director General of Threats, National Crime Agency, Chris Bell, Service Delivery Director, City of London Police, and DCI Clare Chandler, Head of Regional Economic Crime Unit, North East Region.

II: Chief Crown Prosecutor Andrew Penhale, Head of the Regional and Wales Division, Crown Prosecution Service, Steve Smart, Joint Executive Director, Enforcement & Market Oversight, Financial Conduct Authority, and Richard Las, Director, Fraud Investigation Service, HMRC.

Written evidence from witnesses:

City of London Police

National Crime Agency

Crown Prosecution Service

Examination of witnesses

Witnesses: Assistant Commissioner Nik Adams, James Babbage, Chris Bell and Detective Chief Inspector Clare Chandler.

Q296 **Chair:** Good morning, and welcome to the Home Affairs Select Committee. This is our continuing look at fraud. The aims for the session this morning are to assess how well reports of fraud are dealt with and whether fraud is given sufficient priority and resourcing by law enforcement agencies; to understand the journey from reporting fraud to prosecution and whether enough is being done to track down and prosecute fraudsters; and to examine the effectiveness of the Government's counter-fraud policies, including the fraud strategy. I welcome our first panel this morning. It would be very helpful if each of you could introduce yourselves in turn.

Assistant Commissioner Adams: Good morning, everybody. I am Nik Adams, an assistant commissioner with the City of London police. I have responsibility for our national work on fraud, economic and cyber-crime.

Chris Bell: Good morning. I am Chris Bell, service delivery director at City of London police, and one of the chief officer team. I look after Action Fraud, the National Fraud Intelligence Bureau, the National Economic Crime Victim Care Unit and overseeing the transformation of those services.

Detective Chief Inspector Chandler: Good morning, everybody. I am Detective Chief Inspector Clare Chandler. I am the head of cyber and economic crime in the North East ROCU.

James Babbage: I am James Babbage, the director general of threats at the National Crime Agency, and I oversee the National Economic Crime Centre and the National Cyber Crime Unit.

Q297 **Chair:** Thank you very much. We have some familiar faces with us again today, so it is good to see you.

Mr Babbage, could you talk about the overall law enforcement strategy on tackling fraud in the United Kingdom and whether that has changed over time?

James Babbage: Probably the first thing to say is that we have an operational system in the UK that we in the National Crime Agency oversee. That works across and beyond law enforcement, engaging the private sector and getting the right balance between pursuing, preventing, preparing and protecting.

There are three key things that we are trying to achieve. We are trying to improve outcomes for victims collectively through advice and support nationally and locally, including responsive investigation where possible. Secondly, to your question, we are increasingly conducting proactive intelligence-led disruptions, whether online, internationally or nationally,

including through national agencies such as the Serious Fraud Office, the Financial Conduct Authority, the intelligence agencies, the regional piece and the local piece. Data is really key to proactive intelligence-led work. Thirdly, we are supporting the designing out of fraud by identifying and prioritising systemic vulnerabilities.

As far as the strategy is concerned, we have been working on three key shifts over the last two, three or four years. The first is the proactive intelligence-led response, drawing on law enforcement and industry leads. The second is an increased overseas response, because over 75% of fraud is partially or wholly overseas-linked, so we need to be engaging with overseas partners to be effective. The third is targeting the cyber-fraud ecosystem because, increasingly, data is stolen through cyber-crime of various sorts, and that data then becomes ammunition that is turned into individual fraud against victims.

Q298 **Chair:** So that I am clear, you hold the ring on all of this—the buck stops with you?

James Babbage: Overall, that is right.

Chair: Overall. Right.

Q299 **Kim Johnson:** Good morning, panel. Chris, it has been suggested that Action Fraud is not fit for purpose and that there is going to be a roll-out of a new system come April 2024. From your point of view, is that going to happen, and will the new system provide better data-sharing opportunities right across the sector for all stakeholders?

Chris Bell: Absolutely. We recognise that Action Fraud had to be modernised and transformed, and we have been working on that programme for the last two years. We are due to launch a replacement service for Action Fraud during 2024. It is likely to be later in the year when we are able to bring those services live. There is a key range of improvements that we might touch on in some of the further questions, but data sharing, using intelligence and doing more to protect, disrupt and get a better idea of the picture are certainly some of the features we are looking to bring into that service.

Q300 **Kim Johnson:** You don’t think that it will start in April.

Chris Bell: It will not be fully ready to go in April. We are implementing some of the changes through this year, so it is an incremental launch. It is likely to be towards the tail end of the year before we are fully live with the new service.

Q301 **Kim Johnson:** We have heard in different panels that criminals have become far more sophisticated in cyber-fraud. Where are the police up to in keeping abreast of the technology and addressing some of the sophisticated systems used by criminals?

James Babbage: We are increasingly engaged in using cyber-disruptive techniques to disrupt cyber-crime. Just last week, the NCA led the

infiltration and disruption of the world's biggest ransomware organisation. Last year, with the FBI, we took down a thing called Genesis Market, which was a forum for criminals to exchange stolen credentials and all of that for use in fraud.

The other half of your question is, how good is our own use of technology to get after fraud? That is where we are doing improvements, and the new Action Fraud service is certainly one of them, but it is an area where we need to continue to be better.

Assistant Commissioner Adams: You have covered the main points there. We see criminals who are using sophisticated tools, but those tools are not necessarily designed and developed by the criminals. The criminals themselves are not cyber experts. As James described, they are buying services, tools and data online from criminal marketplaces. The focus across law enforcement is on how we identify, through some of the operations that James described, the enabling criminals, some of whom are overseas. There is lots of work with overseas law enforcement in places like Ghana, Nigeria and India to try to tackle, effectively, the head of the snake so that we can stop the proliferation of some of those tools for victims.

Chris will no doubt come back to this, but in terms of the design and development of the new Action Fraud system, the brain that will sit behind it will make it much easier for us to identify the patterns and trends in the technology being used or in things like IP addresses—the sources where people are using that technology. We can then, with a much more pinpoint focus, target our law enforcement response where the source of the problem is.

Q302 **Kim Johnson:** Is any training of police officers on the technology that is required happening at the moment? We are seeing a massive increase in online and cyber-fraud, so do we have the resources available to challenge it?

Assistant Commissioner Adams: There are two points in that. One is about training our existing resources. Yes, we are doing that. In the City of London, we house the national Economic and Cyber Crime Academy, which provides training across the country. We delivered training to over 1,000 officers in the last year. There is a whole variety of courses, but it is about things like the changes in legislation around cryptocurrency and making sure that officers are better able, right from the frontline, to spot where cryptoassets might be stored and seize those, right through to the investigators who will work on those cases.

The second part is the opportunity and the challenge of getting people with the right skills coming into law enforcement. We are running a number of pilot schemes this year as part of our workforce strategy to bring young people, some direct from university, on to schemes that will train them as cyber detectives. They will bring with them the specialist

skills they already have as young technical experts, and we will immerse them in our law enforcement and then work out how we retain them.

Some of that is about the approaches that we need to take to neurodiversity. We know that lots of people who are very tech savvy, particularly those working in a cyber-landscape, are neurodiverse, so it is about making sure that our recruitment and support for people help us get the people with those skills into our organisations and enable them to flourish.

So there is loads of work on getting the right people in and also loads of work on training those who are already in our system.

Kim Johnson: I am glad you mentioned the workforce strategy, because I am sure that will be picked up by one of my colleagues. Thank you.

Q303 **Chair:** Could I be clear on the workforce planning? That is City of London's workforce planning that you are talking about?

Assistant Commissioner Adams: The City of London, as the national lead force, supports all forces throughout the country to improve their capability and capacity on the fraud and cyber response. Within workforce planning, we are looking at the skills we need right across the country. We are looking at the pressures on those skills—what other companies and agencies domiciled in different parts of the country might, through their own recruitment, put unique pressures on policing in different parts of the country—so that we can tailor the recruitment and support we need throughout. For some of those schemes, like internship programmes and apprenticeship schemes, City of London police will support the whole of policing across the UK to roll them out.

Q304 **Chair:** One concern the Committee has is about workforce planning for the future and ensuring that policing has the skilled people it needs. In your role in the City of London, taking the lead, are you able to say to chief constables, "We think you need to go and train up x number of specialists in this particular area," and they do that, or is it discretionary on the chief constable?

Assistant Commissioner Adams: There are lots of things there. Yes, at the top level, that is exactly what we are doing, and it is our ambition to continue to grow that. Of course, there is a plethora of roles. There are new emerging threats that we are trying to track through the workforce recruitment skills that we will need going forward.

Yes, there is some discretion on chief constables. Where possible, we are working with the Home Office to look at how we consolidate some of that funding and offer funding to all forces to bring in certain skills in certain roles.

We are also looking at some of the national schemes where we might work with the private sector to bring in things like forensic accountants

across the country—again through consolidated investment into a partnership that then results in resource being shared across the country.

In our role as the national lead force, building what we refer to as the economic and cyber policing headquarters, a key function, alongside performance and business planning across the country, is making sure that we understand the workforce challenges and needs across the country and that we support forces to develop the response.

Q305 **Tim Loughton:** Why is the City of London the lead force on fraud?

Assistant Commissioner Adams: I have been with the City of London for two years, and I suspect that the answer to that question goes back many more years. The City of London police developed expertise, being domiciled in the City and dealing primarily with economic crime over many years in the City. It developed expertise that was drawn upon by other forces and subsequently as a force it has sought investment to build those capabilities. Over time, and with real logic, that has brought together a range of national portfolios, such as the cyber-crime portfolio and the wider financial investigation portfolio, so that they are consolidated in one place. Instead of NPCC leaders dotted all over the country trying to corral capability and capacity under those portfolios, we put them in one place. A series of decisions were made much before my time on investment in the City of London to build those capacities and capabilities.

Q306 **Tim Loughton:** The City of London force is quite a small force; it is a specialist force. Financial crime in the City of London is largely based on big amounts of money. Why would the City of London police force be remotely interested in my little old lady constituent who has been defrauded out of a few hundred quid?

Assistant Commissioner Adams: I suppose the first thing to say is that we are, because of our national role. I do not know how we got to the place we are in now, where the City of London has had those national responsibilities over many years—I came into the agency two years ago from counter-terrorism policing—but it is absolutely passionate about protecting victims of fraud across the country. It has spent many years building specialist capability, support, co-ordination and training for the whole country, and we have got to a really good place. Ultimately, in the same way as for counter-terrorism policing, a single agency in the UK for policing is needed to provide support and co-ordination, so that there is consistency across the country and our skills, our protect messaging and our crime prevention messaging are consistent. We also house Action Fraud, as the national reporting centre, which then acts as a central repository for all that data around every individual victim, allowing us to understand the patterns and trends and what is needed.

Q307 **Tim Loughton:** I do not disagree with that. What we have been finding in this inquiry is that it is quite hard to pin down where the buck stops with fraud—the interrelationship between your constabulary, as the lead

constabulary, the NCA, Action Fraud and individual constabularies. The fact is that 40% of crimes are now to do with fraud—it is by far the largest sort of crime—yet we have only a 1% prosecution rate, which suggests it is not being taken very seriously at the sharp end, where our constituents are the victims of everyday fraud. It is about trying to get these lines of communication. I will come back to you in a minute, Mr Babbage, on the international dimension of all this.

Can I take a real-life situation, although I will make it hypothetical because there is probably a criminal investigation going on now? Last week, a utility company that covers my constituency was a victim of cyber-fraud, and a potentially substantial number of my constituents and others have had their personal bank account and other details compromised. As a result, this utility has sent out something like 120,000 emails to customers and offered them a free subscription to Experian credit data as a way of monitoring if there is any suspicious activity on their accounts in the future. To most of my constituents who have written to me, and to me, that sounds woefully inadequate. Could somebody give a rough explanation of how that sort of cyber-attack happens and what the potential implications are? What is the involvement of any of the agencies that you represent, or other agencies that are not here, in working alongside that unnamed utility company to try to make safe the existing accounts, catch the culprits and deter use of that sensitive information? Can we have a hypothetical talk through of what happens now?

James Babbage: I will make a start and then hand over. Cyber-attacks like this are, sadly, on the rise and cyber groups, almost exclusively based overseas, very many of them Russian-speaking, seek to disrupt companies, perhaps by encrypting their data or simply stealing it and then holding them to ransom over it. I do not know if either of these has happened in this case or if it is hypothetical, but this happens all the time. As I indicated, part of the way that that data is then used in fraud is by being available through marketplaces and the like.

The first thing that we are doing is disrupting the ransomware groups—there was a very good example of that last week, as I said—and the broader cyber-fraud ecosystem where that sort of data is held. I have some numbers here on the Genesis Market takedown. Last year, there were 75 million credentials and 2 million victims, and UK fraudsters used that data to target 67,000 victims. There were over 100 arrests globally, 34 of them in the UK. More importantly, many of those credentials—these will include credit card numbers and the like—were repatriated. That means that the credit card company was tipped off that they had been found in this way, so it can take action to prevent their fraudulent use.

Much more generally, before I pass on to the broader victim care approach—both the utility company and the customers of the utility company are victims, so there are two different victims here, and City deals with both—there is the prevention work we have been doing to

design out fraud. The reason why we think that card-not-present frauds have significantly declined over the last year or two is initiatives such as the two-factor authentication that you often have to do now. When you use your credit card to make an online purchase—when you are not there with the card—a text message will often be sent back to you with a special code you have to type in. So your constituents, other customers of the water company or whatever do not have to be—

Tim Loughton: I did not mention any particular utility company.

James Babbage: Apologies—utility company. Those people do not have to be as worried as they might otherwise have been. The second point is that the company will have their back.

Q308 **Tim Loughton:** To be fair, the two-code verification happens in a small number of purchases online now.

James Babbage: It happens when the company initiates it. They do that on the basis of an algorithm that is partly about the value of the purchase and partly about other data that they have about the risk.

Tim Loughton: The percentage of purchases made online that require a two-code verification is probably in single figures.

James Babbage: That is probably right, but the number of card-not-present frauds is reducing reasonably fast.

Q309 **Tim Loughton:** Sure, but as it stands at the moment—it may be in a few years that this has changed—the vast majority of purchases online can still just require you to put in your details. In the case of the utility company, some fraudulent criminal gang has now got hold of those and a two-code verification will not be required for them to use those credit card details fraudulently.

James Babbage: In principle that is right. It is also the case that the vast majority of such payments are not fraudulent. The banks, credit card companies and the like are strongly incentivised to ask for that two-code verification in cases that are more likely to be fraudulent, because they pick up the tab when the constituent reads their credit card bill and says, "That wasn't me."

Q310 **Tim Loughton:** Mr Babbage, I understand that, and I understand that it is a desirable move that we should make. But, as it stands, over 90% of transactions are not carried out on that basis, and that figure will remain high for some time to come. I want to deal with the real-life situation now that the credit card details of thousands of my constituents are potentially in the hands of somebody who can use them online fraudulently without second-code verification being required, which could prevent them. Whatever those constituents may be told to do for the future is academic because now they are exposed. What do they do, and how do any of your agencies swing into action, to try to reduce the harm that may be about to happen?

Chris Bell: I will pick up on the elements of the utility and then switch to the victims and talk through that particular journey. The utility company, having reported through Action Fraud, would be pushed into our enhanced cyber reporting service. This is an interim service that we put in place until our new service launches, recognising the differences between cyber and fraud in terms of the crime types, and servicing the business community. That would be assessed. It would be dealt with in swift time and allocated out to the relevant agency—probably the National Cyber Security Centre in this particular instance—to help the utility company close down the cyber-attack.

The victims reporting in would come through the more standard journey. They would come in either through our contact centre or through reporting directly through the web as it currently is. The first step is that we would assess their vulnerability. That would be looking to see if there is any specific care that they need to assist them. That can range from people who are non-vulnerable but who we would give advice on how to improve their security posture, how to get their money back that sort of advice, through to people who might be suffering health incidents and who would get the appropriate care given to them.

We assess the information that is provided for its suitability. That could be pushed through to a local force for investigation and to pursue. We would use the information provided for further prevent and protect and to get that messaging out locally and nationally on the incident and what is happening. We would try to make sure that people do not become further victims and are not exploited by the information that is out there.

The third bit, as James touched on, is using the information to disrupt the bad actors. That is the premise of what the National Fraud Intelligence Bureau is there to do and what we will be in a far better place to do more effectively when our new technology solutions kick in this year.

Q311 **Tim Loughton:** Do you think that the utility company should be doing more than just offering a free subscription to Experian's enhanced credit checks?

Assistant Commissioner Adams: For the individual victims in that case? I do not doubt for one second that they will be doing an awful lot in the background. As Chris alluded to, the first and most important thing for us is that the company reports to Action Fraud the fact that this has taken place. That then triggers all this further activity, at national level, regional level or local level, from the local cyber-crime team, to help with the investigation.

There is also the partnership we have with the National Cyber Security Centre, helping the company to lock down their data, check whether they are secure. Often, as a result of companies' insurance policies and relationships with private sector support, there are quite significant delays in us finding out—if indeed companies ever come forward without

us finding out on the news—that certain cyber-attacks have taken place. That then delays all that additional work that we can put in.

One thing we would expect to take place is the identification of those details and work with individual victims and their banks to make sure that, if there are credit card details held within the utility company system, those credit cards are effectively shut down so they cannot be used for online payment in the way you have described. Then, of course, Experian is offering people the ability to monitor whether their broader personal data is being used to obtain credit in the future. We see day in, day out, with the data that people put on social media and the stuff we are sharing when we make online payments, sometimes to individuals for things we are buying on marketplaces, that immense amounts of our personal data circulates around criminal marketplaces because it is gathered by criminals and is sold as packages for other criminals to use.

The biggest way we will stop some of this is, as James described, through the work of the banks to make sure that people's data is protected, that people have advice and are monitoring their transactions, and that where data is stolen—particularly individual credit cards—that is shut down so that it cannot be used by a criminal going forward.

Q312 **Tim Loughton:** DCI Chandler, you are getting an easy run so far, so I will come to you. If my constituent, or a constituent in the region that you cover, found that fraudulent activity on their bank account or their credit card that is likely to have come from their data having been pinched from this utility company, do they go to the local police, Action Fraud or the utility company? Where is the chain of reporting and support for the individual who has been the victim of a group fraud?

Detective Chief Inspector Chandler: It would not necessarily come direct into policing, because of the Action Fraud reporting system. However, people do ring policing to report those types of frauds, and they will be advised where to take their report. Once it comes back out to policing, policing can seek to investigate individual frauds. It may come to a regional perspective, depending on the severity of the fraud, or it may go to the local fraud investigation teams to investigate them. However, the process is still there to report through Action Fraud and to then come back out to either local forces or regional teams.

Q313 **Tim Loughton:** If there has been a big group action, it would presumably be useful for investigation purposes to be able to link different customers who have been fraudulently attacked, because their data came from the same place. How would that link up? If my constituent says, "Somebody has used my details to purchase this online," and another constituent comes and says, "My details have been used to purchase this," how do you join that up? Who joins that up?

Chris Bell: That is the role of the National Fraud Intelligence Bureau. We take the reporting in from Action Fraud and UK Finance, and we are looking to strengthen other reporting mechanisms. We connect and

analyse the victims. Where there are linked crimes, we will put them into bigger packages. We then disseminate that out to either the regions or the local forces. That work is done, and that is the strength of having the central area—we look at all the reports coming in and see the linkages back to specific actors or specific crimes and actions that have happened. That is how we pull those packages together.

Q314 **Tim Loughton:** How will you know that those individual constituents were customers of this utility company that has been hit?

Chris Bell: It will depend on the information that we are provided with by the utility company and what the victims have reported in. From the information that we pull together, we will see where there are linkages and bring the packages of work together. That is the work we do.

Q315 **Tim Loughton:** Will the utility company give you a full list of all its customers whose data has been compromised? If you then get an individual report from Mrs Miggins, who is on that list, or Mr Smith, who is on that list, will you make that link? The utility company has hopefully given you the list of all the people involved.

Chris Bell: That is the ideal position—that they would present all the potential victims to the crime in through that central report from the cyber-attack. Obviously, we would link anyone who reports individually that they have been a victim back into that.

Q316 **Tim Loughton:** If they have not done that?

Chris Bell: We work with the information we have been provided with.

Tim Loughton: But if they have not done that, there is a duty of care on their behalf to have done that, yes?

Assistant Commissioner Adams: It does not sound unreasonable. I would say yes.

Q317 **Tim Loughton:** I do not know if they have done that or not. It is one of the many questions that I have to ask them. I have an awful lot of constituents who say, "I have been told that my details have been taken," and who then receive another notification saying, "Your details have not been taken." There is complete confusion here. I want to understand how this chain of reporting and supporting subsequently happens.

Mr Babbage, you said that 75% of fraud originates overseas or is linked to overseas. We were given the figure of 70%, but it is around three quarters. How do we know that?

James Babbage: We know that from all the work that we do to look at different fraud types.

Q318 **Tim Loughton:** What does that mean?

James Babbage: The crime survey of England and Wales does work that tots up how many different frauds have happened. We look at the different types of fraud and we look at what we know about criminal behaviour. That is where that figure comes from. I cannot give you a detailed description of the methodology that produces that number. We are talking about where the suspects are, where services and infrastructure are provided. A lot of different overseas elements come into play.

Q319 **Tim Loughton:** I have been the subject of fraud on my credit card two or three times—each time for purchases of teenage dresses, for some strange reason. How would I know if those are foreign-linked or not?

James Babbage: You would not, and this is very much the point. In about a third of cases, the victim of fraud may have been in touch with the fraudster, and in two thirds not. In only half of that third do they have any useful information as an individual victim to pass on to Action Fraud. This is why the proactive intelligence-led response is such an important part of the strategy that we are collectively following.

The new national fraud squad is the proactive part of all our operations. It has started off about 250 strong and will grow by 400 by the end of next year, and it is now about two thirds of the way through that growth. That is going after cases where we have technology that is being used in a particular way to enable frauds at scale or after other fraud patterns, so that we can disrupt fraud at a much greater scale.

Let me give you an example linked to overseas work. NCA has outreach in about 130 countries globally. If you go back to 2019, we had eight disruptions where fraud was the primary issue at stake. Two years later, we had 25, and two years later again we had 183. So nearly 10% of our international work is now fraud-related.

In that time, fraud has reduced a bit, which is good, but part of the reason why fraud has reduced is that we are beginning to gear up this strategic, proactive pursue response, which is not dependent on individual victims reporting in the little information, exactly as you say, that they have about specific frauds. It is much more dependent on this intelligence-led approach of understanding how fraudsters are committing frauds at scale.

Chair: I am going take Carolyn and then Alison, who have two short questions that have arisen out of Tim's questioning.

Q320 **Carolyn Harris:** Given the sophistication of the ability of these fraudsters to infiltrate one's phone, which has happened to me and many people I know very regularly, how much are we picking up in what is being reported? Are we just reaching the tip of the iceberg? My son had a text from a delivery company last week—he was expecting a parcel from another delivery company—saying he needed to pay blah-di-blah. He did not report that to the police. I had one last week that came on a thread

from my bank saying that I had made a transaction and asking if I would confirm it by pressing a link. I thought, "Well, that's never happened before," and I phoned my bank, but if I was an elderly person or someone who was not quite as informed, I probably would have done that. Are we missing more than we are picking up?

James Babbage: I think that the crime survey of England and Wales approach is useful because it does not rely on looking at how many frauds have been reported. It relies on reaching out proactively to people randomly through the country and asking them about their experience. In that case, even if you had not taken any particular action, you would talk to them or fill in their surveys or whatever. That is why I think the crime survey of England and Wales is a good source of numbers.

Carolyn Harris: They have never called me.

James Babbage: I have never been rung up by a pollster either, but I rely on political polling and opinion polling as having some scientific basis.

Q321 **Carolyn Harris:** How does they do this survey that you talk about?

James Babbage: In the same way as opinion polling. They will have a scientific basis for working out a representative sample of the country from right across the country—different demographics and all of that.

Detective Chief Inspector Chandler: From a regional and local perspective, we also have engagement teams. When there are trends identified, our engagement teams will go out into the public and engage with the public to warn them what the current trends are. They are becoming more sophisticated, so it is difficult. In the north-east, we have an engagement team in cyber under the three Ps—protect, prevent, prepare—and the same in fraud, and we are reaching quite high numbers of the public. We engage with all different age ranges through Age UK, visits to libraries, universities and schools. When these trends arise, we will go in and support members of the public so that they can understand the reporting processes, should they be a victim.

Q322 **Carolyn Harris:** Do you proactively target people like Age Concern?

Detective Chief Inspector Chandler: Yes.

Assistant Commissioner Adams: All of this is predicated, as you have described, on people reporting things to us so that we have the big picture of the data. We recognise, as the Home Office does, that we do not get full sight of all of those reports. We want to be able to take the email and text message that you have, do the analysis of it, work out where the IP address is that that has been sent from and then, working with other law enforcement partners, do some disruption work on that. If things are reported and forwarded on to the NCSC reporting line—some of that work is now increasingly automated—that work takes place.

The entire premise of the new national Stop! Think Fraud campaign that was running on television last week is about raising awareness of the situations that are created for people, where you are put under pressure to make a quick decision to authorise something or to pay some money. The campaign is about helping people to recognise the situations they might find themselves in that are fraudulent and to take action to stop that. A website sits alongside it that tells people how and where to report.

Increasingly, the next bit, which is really important, is that reporting. The new Action Fraud system, in its incremental development over the next few years, will have the sorts of technology behind it that will allow us, through the automated sharing of data with social media companies, tech companies and telephone companies, to take disruptive action against the perpetrators of those crimes and stop the next person from receiving that information.

It needs a whole-system approach. As Clare described, at the centre we can identify what the patterns and trends are; work out what the demographic and the age groups are, in what part of the country, and what people's likes and interests are; and then reach out to them through things like Age UK, local neighbourhood policing teams or the dedicated protect officers, who go out and meet and help people understand specific threats that might be most relevant to them.

Chris Bell: If I could add one piece, that is the difference of the new service that we are bringing in. It was very much built around the pursue activity. That will remain and be strengthened, but this is about industrialising that protect information, being able to take the data at scale, share it out and get the public messaging out, and getting disruption notices out to industry so that the repeat victimisation through these types of scams is reduced significantly. A key part of our design is being able to deal with that data and to analyse and push quickly. At the moment, a lot of that stuff is done almost manually, and the longer it takes, the less impact it has when we get that educative information out through the various networks.

Detective Chief Inspector Chandler: In the pursue activity, we quite often identify further victims that we were not aware were victims in the first place. We are proactively approaching people through other investigative techniques and identifying members of the public who are unwittingly victims of fraud.

Q323 **Alison Thewliss:** Scotland does not use Action Fraud, presumably because it is not very good. Could you tell me a wee bit more about what the plans are for communication with Police Scotland about the new project that you are working on to replace Action Fraud? I know that the NCA is a partner in the Scotland Crime Campus at Gartcosh. Could you tell us a wee bit more about how that works for fraud?

Chris Bell: I will take the Action Fraud side of things. Since we have been preparing and building the business case to replace Action Fraud

nationally, we have been engaging with Police Scotland. They have sat on the service board and the design boards, so they are aware of everything that we are looking to do. We are putting the infrastructure in place for it to be able to operate in Scotland in respect of some of the different accounting rules and different judiciary provisions in Scotland.

We have been looking at how we will deliver the service and what benefits it will bring to Police Scotland. Police Scotland is now looking at that in terms of a business case that they are providing. Dialogue is ongoing and positive. Police Scotland been involved in all of our testing, and we are getting them involved in user testing of the new system so that they see it in action.

We are very keen to have Police Scotland. We think that it is important to have a full national threat picture on all the frauds. We believe that we can assist Police Scotland with the dissemination and the tasking of those crimes. We are working with them on that, but ultimately it will be a Police Scotland-led proposal, which will come through the appropriate channels. However, they have been fully engaged, and that has been key, because we see it as an important step in having a UK picture.

James Babbage: We work with Police Scotland at Gartcosh, and they have the same proactive approach that we have been describing here. There will be operations that they see the need for and take forward and that we will advise on. Perhaps if there are international aspects of those, we will work with them. I gave the example of Genesis Market, and there will have been victims and, potentially, criminal users of that in Scotland, so that is fully taken care of.

To add another point, from time to time we run an annual intensification, focusing on a variety of frauds. We are in the middle of one at the moment. The very first week we saw 77 arrests and a whole number of asset-freezing orders and confiscation orders. I do not have the data on how many of those were in Scotland, but Police Scotland is certainly playing into that activity.

Q324 **Alison Thewliss:** Are there useful linkages there with the Serious Organised Crime Taskforce in Scotland so that frauds do not just appear as a small blip on somebody's bank account but are part of a wider picture?

James Babbage: Yes. There is this whole intelligence picture of building up intelligence from victim reporting but also from what we understand criminals are doing. Partly we see the proceeds of frauds through our illicit finance work; that can be another way in. We are about to launch a fraud-targeting cell. That will essentially allow us to improve on the current insights that we have and to develop those insights into much more fully developed intelligence packages that can then be investigated, whether in Scotland or elsewhere.

Assistant Commissioner Adams: Police Scotland are very much part of our national network. It is genuinely by huge coincidence that we have a team of officers from the City of London up in Scotland today, working with colleagues there on the back of work that we do through our national role to visit every force in the country, to look at best practice and to consolidate that into the new national strategy we launched in November. We see part of our role and responsibility as going and making sure that, wherever possible, everybody is using and sharing that best practice, reviewing everything from governance to how performance is managed, to investigations, to how intelligence is collected. That is what we are up in Scotland to do today.

Q325 **Chair:** Can I ask a general question? We acknowledge that there are problems with reporting to Action Fraud. If someone goes to the trouble of reporting, why is it that, at the other end, we are not seeing the number of investigations, prosecutions and convictions? Where in the system is this falling down? If you do report, you are packaging up the case to go to the police force. Is it at that level? It goes back to the police force and it is not given any priority; is that where the problem is?

James Babbage: It is important to be clear on whether the main thing is more criminal convictions in the UK.

Chair: For this Committee for today, let's say that what we are interested in is bringing people to justice who are committing fraud. On that basis, why are we not getting enough prosecutions and convictions?

James Babbage: There is definitely a story to tell about what happens in the UK, and I will defer to colleagues on the detail of that. Many of the people who are committing these frauds are doing so from overseas. Even where we work with foreign partners to prosecute them, which we absolutely do and are increasingly doing, that will not end up in the statistics for a conviction in the UK. That is the first point.

Q326 **Chair:** You said earlier that 70% have an overseas element. Why are we not seeing higher levels of prosecutions and convictions for the 30% that do not?

James Babbage: The second thing is that the proactive intelligence-led work that I have been describing is still in its relatively early days. I can see what we call the intelligence pipeline really increasing in volume. The number of investigations at the moment is healthy but is not increasing yet, because the intelligence packages are not developed enough and not mature enough, although the system is maturing. As the rest of the national fraud squad is built, we need to see greater investment in the investigative side as well as the intelligence side. Then you will start to see more prosecutions come through the system.

Q327 **Chair:** You do not think that police forces are the problem—that they are not giving any priority to this? That is not the problem?

Assistant Commissioner Adams: I am happy to answer that. Across the country, there are probably 1,500 dedicated specialists investigating and dealing with the other aspects of fraud. That is clearly nowhere enough to be able to deal with the volume and scale of offences.

There are, of course, significant challenges because of the overseas issues and the way in which people use technology to disguise their location and use muling to transfer money through multiple bank accounts before it gets to the offender in the end. That makes it very difficult and complex to investigate those cases.

With the resources that we have across the country—Chris will talk through some of the numbers—we try to make sure that we prioritise the cases that have the greatest lines of viability and that are most likely to result in somebody being identified and the potential for prosecution, alongside identifying the victims who are most vulnerable. That is generally the victims against whom the most harm has been caused. With the available resource, we prioritise those cases accordingly. However, it is technically difficult to get the prosecution levels that we want, for a whole host of reasons, as we said. Also, from a resource capacity point of view, there is a limit to the number of specialists at the moment.

We hope that the strategic policing requirement that was introduced last year will make a difference. The work that we have been doing—going around the country and working with forces, as I described before—is focused on making sure that fraud features in police and crime plans and in mainstream police performance, with chief officers holding teams to account over mainstream police performance.

Through the work that we have done to set up the national policing strategy, there is very much local investigative activity that can be undertaken. As James described, a proportion of frauds take place face to face between local offenders and local victims. We need to make sure that mainstream local policing is picking up those cases.

There is a lot to do, and there is a lot that we are doing to drive up those outcomes, but we fundamentally believe that the biggest impact we will have is in drawing all that intelligence together to identify the biggest enablers of fraud and then in using partnerships across policing, the NCA, globally and the NCSC to take down and disrupt those enablers. At the core we have serious organised criminals creating a massive volume crime impact on local victims.

Q328 **Chair:** I am interested that only 1% of police resources are dedicated to fraud. If you are going to do all of that, what percentage of police resources will be needed to deliver what you say you want to do? Are you going to go from 1% to—

Assistant Commissioner Adams: There is a range of things there. There is the things that are dedicated to fraud. The numbers that I was

talking about are specialist investigators. We do not know how many local investigations in local CID teams or neighbourhood teams involve fraud, where you have other officers engaged.

There is something fundamentally about continuing to upskill police officers and police staff investigators across the country to investigate this stuff at all levels of the organisations. I cannot give you an exact figure for what the proportion of police resource going into specialist roles should be. Indeed, growing that capability and capacity, even with immediate investment, would take several years because of the time it takes not only to recruit and train people but to then mentor and assimilate them into teams. There is only limited capacity to continue to grow specialist capability.

Q329 **Chair:** Is there a timeframe? You say that fraud is 40% of crime in the UK, and it is only getting 1% of police resources at the moment. Do you have a five-year plan that will allow you to say that, by 2030, we will see 10% of police resources spent on fraud?

Assistant Commissioner Adams: I am not in a position to mandate to police chiefs how much dedicated resource they put into fraud.

Q330 **Chair:** It is up to them; they can decide?

Assistant Commissioner Adams: To a degree. Some of it is dedicated, ringfenced funding that comes from the Home Office into specialist teams, which then ensures that there is a minimum capability. Beyond that, it is the prioritisation by police and crime commissioners and police chiefs at a local level that decides what they put in.

Where we want to get to through all the work going on with things like the online fraud charter and the Online Safety Act is to see how much of the volume we can take out of the system through the disrupting of criminal enablers. Over the next few years, that will give us a much clearer picture of the remaining offences that can be prosecuted—that we can investigate and get to a prosecution—and that will give us a fundamental answer to the question of what our five and 10-year ambition should be in terms of growing the specialist teams and capabilities we need in the UK.

Q331 **Chair:** DCI Chandler, we had some evidence from the Police Foundation, which recommended that fraud investigation should be lifted out of local police forces and assigned to dedicated regional units. What do you say about that?

Detective Chief Inspector Chandler: We have seen uplift anyway in the regional units. The forces have their own representation in economic crime investigation of lower-level fraud investigations. However, we have seen significant uplift in funding into proactive economic crime teams. Historically, we have responded reactively to fraud, but we are now in a better position to respond proactively.

Regionally, we also have other capabilities that can assist in those investigations, such as undercover online, undercover operatives, high-harm investigation teams. We are seeing the benefits. However, we still have challenges in recruitment and retention of officers and the training pathways. If we are taking in somebody who is untrained—for example, a financial investigator—that pathway can take up to two to three years, so it will take time.

Q332 **Chair:** Do you think it is right that police forces themselves are still dealing with this? You do not agree with the Police Foundation that it should go to a regional unit?

Detective Chief Inspector Chandler: My personal view is that we would be deskilling police officers in certain areas of business. Personally, I think that forces should still manage.

Q333 **Chair:** Do you think they are doing well?

Detective Chief Inspector Chandler: They do not have the same resources or their priorities differ. Control strategies differ nationally. Support-wise, they could also do with some support—funding uplift—in that area of business.

Q334 **Tim Loughton:** Mr Babbage, given your name, I presume you are au fait with computer technology. Who is going to benefit more from AI, the fraudsters or law enforcement?

James Babbage: In the first instance, the absolute risk is that the fraudster does. The crimes that we see growing the fastest are those that happen over the internet. Potentially, victims in the UK are opened up to criminals throughout the world and where the criminals can automate the earlier stages of that process.

However, it is important to remember that we are winning on fraud and we are bringing it down. Even though I think that the underlying risk overseas is probably growing, all the work that has gone on since the original NCA crime and courts Act ask in 2019 and then, under the economic crime plan 2, the additional Home Office investment, as well as the growing of the national fraud squad, and all the strategy that we have set out to you today, has brought the overall fraud numbers down from their pre-pandemic level by something like 13% now, despite the fact that there was a bump in covid.

There is lots more to do. When I was here before, you asked what was my one recommendation, and it is about staying the course and ensuring that we continue to grow the national fraud squad and, particularly, that we continue to get new investigators in, now that we are growing the intelligence pipeline. We need to get to a position where AI is enabling our response as much as it is the fraudsters.

Q335 **Chair:** Do you think that businesses are able to report to Action Fraud easily? I have heard that they find it very difficult.

Chris Bell: It is a challenge that we have. They can report. We have a bulk reporting facility that we are looking to strengthen and make far more tailored to different types of victims as we work through. There will be different user journeys and different ways to report into the service, and that will be tailored to circumstances. Businesses, different types of victims, and large-scale, bulk upload coming from industry—we are looking to be able to take all of that information into the new service.

Q336 **Chair:** Will this all be available by the end of the year?

Chris Bell: This will be incrementally coming into place from later this year.

Chair: Explain to me what that means.

Chris Bell: We are building a service to go live, and then we will continue improving and adding enhancements to the service so that we can get the new world live while we continue to build enhancements in the background.

Q337 **Chair:** You are starting it off at the end of the year, but you are going to be adding on bits.

Chris Bell: Absolutely.

Chair: When will you actually have a functioning Action Fraud reporting service?

Chris Bell: It will be live later this year.

Q338 **Chair:** When will it have everything it needs to be effective?

Chris Bell: It will have everything that it needs to be effective from day one. We will continue to enhance from the experience and the feedback that we get from users, so that there is a continuous improvement in the service. One of the biggest weaknesses of the current service is that it was launched and it has been the same—it has been static—for six or seven years. We will take the feedback, continually improve the service, add new features, link in with different data-sharing agreements in other parts of industry, where agreements or legislation allow. It is being built to be scalable and to be continually improved and adapted to the way that people want to report as we go through the life of the service.

Q339 **Chair:** From the end of the year, businesses will be able to report in a far easier way that meets the needs that they have, and you will be improving the service as you go along in future years?

Chris Bell: Absolutely—taking the feedback of the users.

Chair: It will be working from the end of the year.

Chris Bell: Yes. We will not go live before it is working.

Q340 **Chair:** We were told April. What is the delay?

Chris Bell: April was an estimate. We are working through the last component parts of that project. Like with any complex service, there is a number of projects that are intertwined. It is going to take us a little bit longer to get to a stage to launch the service. It was the ambition to launch in 2024. We believe that we will do that. We have just not been able to achieve the April date, which was our original target back in 2020, when we started the journey.

Assistant Commissioner Adams: Given the history of Action Fraud, we want to absolutely get the new system right before we launch it. There is nothing worse, for all the reasons that we talked about before on public reporting and business reporting, than people losing confidence in it from the outset.

I know that the premise of your previous question was the focus on us finding people and prosecuting them, but one of the big things the new system will give us is the ability to deliver a whole range of other outcomes for victims. That will involve everything from out-of-court outcomes to getting low-level offenders into programmes where there are opportunities to divert them away from cyber-crime or fraud engagement, particularly on things like money-muling, where individuals allow their bank accounts to be used by criminals.

The focus for us in the way that we are building our national performance is to understand much better the range of outcomes from all the stuff that Clare talked about around prevention, as well as prosecuting and disrupting offenders, so that we can understand these things better.

Chris Bell: That adds on to the fact that we cannot just rely on investigating our way out of it. We need alternative outcomes, and that is what we are building—that protect, that far better disruption and that taking down of the assets that are used. Altogether, working with better packages and the investigative power growing, should see us continue to—

Chair: This all sounds good, but we are all very conscious that fewer than one in seven fraud offences are reported to the police or Action Fraud at the moment, so there is a huge job of work to do. Obviously, one very clear thing is to see people being brought to account and being brought to court, prosecuted and convicted. That is something that we would all like to see where possible.

Thank you very much for your evidence today. We will move on to the second panel now.

Examination of witnesses

Witnesses: Andrew Penhale, Steve Smart and Richard Las.

Q341 **Chair:** Welcome to our second panel this morning. I will ask each of you to introduce yourselves to the panel.

Steve Smart: Thank you and good morning. My name is Steve Smart. I am one of the executive directors of enforcement at the Financial Conduct Authority.

Andrew Penhale: Good morning, I am Andrew Penhale, a chief crown prosecutor in the Crown Prosecution Service. I head up a team of prosecutors engaged in serious economic and organised crime prosecutions. I am the economic crime lead for the CPS.

Richard Las: Good morning, I am Richard Las, the director of the Fraud Investigation Service in HMRC.

Q342 **Chair:** You are very welcome. You perhaps heard some of the questions that we put to the first panel. I will start where we just left off. One thing that concerns me a great deal is the number of fraud offences that are being committed. We know that it is growing overall. Those people who do manage to report what has happened are very dissatisfied with what happens next. So few cases find their way through police investigation to court and to conviction. Could someone explain where the problem is? Is it that the police are not investigating and not giving this priority? What is the problem? Why are we not seeing more convictions?

Andrew Penhale: The initial problem is the scale of fraud across the country. You heard from the NCA and City of London police that the number of fraudsters across the world targeting individuals in the UK is immense. I should say that it is not just the police who are investigating fraud; there are a number of other agencies. HMRC is here today, and the Financial Conduct Authority, but there are various other strands within Government. The NHS have a team of prosecutors, DWP have a team of prosecutors, and there is a range of different agencies involved in investigating fraud, all of whom feed into the system.

However, the scale of the problem is huge. It is right that a lot of the focus of law enforcement's efforts is on prevent and protecting the public, rather than just on pursuing individuals and prosecuting them. Clearly, the numbers need to be increased—public confidence requires that. All of us who are involved in investigating or prosecuting are absolutely passionate about it; we want to bring criminals to justice, to mark their cards and demonstrate to the public that we will do that.

Ideally, we want to strip criminals of their assets and gains and return those to the victims where we can, and we have had some success in recent years. The CPS have taken in excess of £400 million off defendants since 2018, and we have returned about £105 million to victims. So there is no shortage of determination to do this.

Q343 **Chair:** Why are you not doing it? You are all determined to get on and prosecute and get convictions. What is the problem?

Andrew Penhale: We do prosecute. In 2022-23, we prosecuted in excess of 6,000 individuals, with a success rate of just under 84%.

Q344 **Chair:** Once they get to you, you are getting them to court—I know that there are huge backlogs in the courts—and getting good conviction rates. What is the problem, though? Why do all these other people never even get to your stage?

Andrew Penhale: As you have heard already, resources have to be targeted in the right area. There are other priorities and other demands on the wider investigative system, particularly in policing. However, the cases that do come through to us generally result in good investigations and good prosecutions. Our charging rate is about 75%, so a significant majority of the cases that come to us result in prosecutions.

It is right, as you heard from the City of London police, that they will target the criminals who have had the biggest impact on victims—those with the largest number of victims or taking particularly large amounts. Inevitably, they have to do that. Part of bringing prosecutions is sending a message out about prevention. A big sentence will have an impact in a business area and make people think.

I cannot answer everything about priorities in wider investigative teams, but, essentially, there is that determination to prosecute when cases are brought forward.

Chair: When they are brought forward.

Q345 **Tim Loughton:** Mr Smart, can I ask you first about the bank checks? In a previous session, I had a query about fraudsters who typically con people into paying money into a bank account, which is then instantly cleared. However, as all of us know, when you try to set up a new bank account, you have to provide your blood type and virtually everything else to go with it. So who is failing to do proper checks against money laundering, as the first port of call, which would enable somebody to fraudulently filter money through a third-party bank account without the bank knowing exactly who they are and how to get it back?

Steve Smart: You are asking about Know Your Customer and doing customer due diligence at the firms that we supervise. As Andrew said, prevent is an important part of our approach to fraud and the team approach to fraud. It is a role that the FCA plays. Alongside that, we investigate and prosecute in the fraud space as well. I agree with Andrew's comments about prosecution. We are not a volume fraud prosecutor or investigator. One of the areas where we really add value is in that prevent space. You are talking about how we best work with the firms to ensure that the KYC and the customer due diligence are of the right level—that their fraud and money laundering controls and systems are tested and of a level that will spot this as it is happening.

In the last six months, we have produced several publications that show some of the work we have been doing with different parts of the financial sector. In 2022 we did an assessment of challenger banks and some of the new firms coming into the system and where they would need to

focus. In November we produced a report on an assessment we did of a series of payments firms, including some of the new electronic money institutions. In that, we could see that some good processes were being employed, but there were some areas where some firms needed to focus more, such as knowing your customer, at the start of the process. Customer due diligence throughout the process is one of the areas that we are working on with firms.

Q346 **Tim Loughton:** Yes, but my question was: how can I set up a bank account without having to prove exactly who I am with a traceable series of utility bills and everything else that you have to provide? How can somebody possibly set up a bank account, effectively, with bogus details that you then cannot trace once the money has left the account?

Steve Smart: It should not happen. It will be a failing of systems and controls, and that is where we need to work with the financial services sector to help ensure that the right systems and controls are in place. You will have seen some big growth in certain areas of the financial sector over recent years. On payment firms, with the EMIs, a lot of new and innovative companies are coming in. It is our role to try to ensure that their systems and controls can keep up with the innovation in the work they are doing.

Q347 **Tim Loughton:** You say that it should not happen, and we know that. Under money laundering regulations alone, it must not happen; otherwise, they have failed to uphold the duty of care on them. So how is it able to happen?

Steve Smart: It comes down to their systems and controls and the ability to verify. When we work with some firms, we see examples where, if you have the right system, you should pick up where lots of accounts are being set up from the same device or from the same address. Those are areas that need to be flagged and looked at. That is the process that we are going through with companies at the moment.

Q348 **Tim Loughton:** In terms of accounts—again, this came up earlier—you may have fraud going through multiple accounts with the same address, and using the same IP addresses as well for electronic communications. You should not be able to set up even one of those accounts without proving that you are a bona fide citizen whose address can be traced to here. I still do not understand how this is happening.

Steve Smart: I will come back to it. It comes down to the systems and controls that the institutions that are setting up the accounts have in place. Where we can see and evidence that those systems and controls are not right, we are working with them to improve them. We will take enforcement action if needed in that space. We look at that, and we are continually—both proactively and reactively—looking at those systems with the companies. The latest review we did looked at 150 companies where we could see that the risk was perhaps higher because we had not had regular contact with them. They were probably issuing less than 10

suspicious activity reports a year. Going in and being able to focus our effort on those companies—I agree with you that it should not be happening, but it is and we are looking at ways to try to—

Q349 **Tim Loughton:** It is no good agreeing with me that it should not be happening. You are the enforcement agency; you are the Financial Conduct Authority. You are all over banks and financial institutions at the moment to enforce diversity quotas and all sorts of other things that have nothing to do with finance, but you appear to be failing in your basic requirement to make sure that all bank accounts that are being set up, which provide profit to financial institutions, are set up by legitimate people with a proper paper trail. Clearly, that is not happening, because the only way this financial fraud can happen is that it is channelled through what, in the vast majority of cases, turn out to be bogus bank accounts. How many bogus bank accounts have been used, roughly, as an assessment, over the last few years?

Steve Smart: I cannot tell you that—I do not have that stat—but I can certainly write to you with that information. As an organisation, economic crime is a priority for us, and trying to stop and reduce economic crime is a priority for us. It is one of three priority commitments that we made in our current three-year strategy, which launched in 2022. As I said at the outset, we focus, from a preventative perspective, on seeking to try to prevent fraud, as well as on a pursue perspective, in looking to have the impactful deterrence that Andrew was talking about and that you were asking about—

Q350 **Tim Loughton:** Mr Smart, with the greatest of respect, usually when Ministers come along and say, "This is a priority for us," it means that it is not a priority for them. Just using words, saying that it is a priority, does not make it a practical priority in what you are doing. Let's have some hard figures. How many prosecutions or penalties have been imposed as a result of your enforcement action against financial institutions in this country for hosting bogus bank accounts that have been used for fraud?

Steve Smart: Again, I will have to get you those figures. As I said at the outset, we are not a volume fraud prosecutor or investigator, but we have done more in the last year in the prosecution space than we have ever done before on economic crime, in general, and fraud, in particular. Of our current live enforcement operations—there are 190 live operations—about 40% are linked to economic crime and 30% are fraud-linked. We have prosecuted 10 people successfully for fraud in the last 12 months. That is significantly more than we did in the three or four years before. But it is small numbers because we are not a volume prosecutor.

Q351 **Tim Loughton:** One hundred and ninety investigations?

Steve Smart: Live operations, yes.

Tim Loughton: Live investigations, 30% of which are for fraud.

Steve Smart: Are linked to fraud, yes.

Tim Loughton: That is 57 or so, and 10 people have been prosecuted. How many bank accounts are there in this country?

Steve Smart: I could not tell you off the top of my head.

Q352 **Tim Loughton:** How many financial firms do you regulate in this country?

Steve Smart: We regulate about 50,000.

Q353 **Tim Loughton:** And you have prosecuted 10 people.

Steve Smart: That is why I said at the outset that we are not a volume fraud investigator or prosecutor. In terms of a lot of what we do in the economic crime space, we are having some success. I caught the end of James's response to you on fraud and whether fraud is beginning to come down. We focus on two particular frauds. We focus on APP fraud, which is what you are talking about with the bank accounts, and on investment fraud. APP fraud has stabilised. If you look at the UK Finance figures for the first half of last year, the value of the APP fraud was more or less the same as in the first half of the previous year. Volumes of offences went up slightly, but it appears to be stabilising.

On investment fraud, we are seeing the rate of growth and the number of losses come down fairly significantly, and we have played a key role as an organisation in that. We do a lot in the prevent space, partly through regulating the financial sector and through the work we do with companies on their systems and controls.

We also do a fair amount of work with social media companies and big tech about identifying scams and bogus investment schemes to bring those down and close those down. We do a lot of work to try to educate customers. We need to focus on all those areas if we are to bring this problem down.

Q354 **Tim Loughton:** How does your enforcement system work? If you have found that a challenger bank or whatever financial firm has been allowing, let's call them, bogus bank accounts to be used in this way, what is the first step that you take?

Steve Smart: We will supervise that firm. We will look at what has caused that to happen—a systems and controls issue or a different sort of issue—and we will open an investigation if that is the right way forward.

Q355 **Tim Loughton:** All right. And what are the outcomes of those investigations?

Steve Smart: There are various different outcomes. It can lead to significant fines, and there have been significant fines against some of these companies in previous years. It can lead to a focus on individuals if

there are some individual failings in there. It can lead to criminal charges if there is evidence of criminal activity.

Q356 **Tim Loughton:** Is it criminal activity by the firm if they have not regulated properly? That is not criminal activity, is it?

Steve Smart: No.

Q357 **Tim Loughton:** Who has committed the criminal activity?

Steve Smart: The fraudster who is moving the money, the money mule or the individuals involved in the money laundering.

Q358 **Tim Loughton:** But we are not talking about employees or associates of the bank or financial firm?

Steve Smart: For a firm, it is liable to end in some sort of fine.

Q359 **Tim Loughton:** Okay. You have investigated a small financial firm and you have discovered a number of bogus bank accounts. You will work with them to say, "You have to improve your systems." You may or may not impose a fine at that stage. Do you come back six months later? Do you do an obligatory follow-up check? How does it work then?

Steve Smart: Yes. There will be reactive and proactive supervision. We will proactively be looking to see if the issues that we have identified have been rectified and if the problem continues or does not continue.

Q360 **Tim Loughton:** What happens if it has not been rectified?

Steve Smart: We will look again to try to understand why it has not been and start another investigation or build on the investigation that we have been doing.

Q361 **Tim Loughton:** What happens then?

Steve Smart: We may end up putting another fine in place, but we want to work with the firms and stop the problem.

Q362 **Tim Loughton:** I am sure you want to do that. At what point does that firm lose its licence?

Steve Smart: That can happen. It depends on the issue and what has occurred.

Q363 **Tim Loughton:** How many of your 50,000 regulated firms have lost their licences in the last few years?

Steve Smart: Again, I will have to provide those figures for you, but we will remove the authority or ability to operate of a number of firms. I cannot tell you off the top of my head how many.

Q364 **Tim Loughton:** It is an important figure though, isn't it?

Steve Smart: Yes. I am very happy that I will provide that figure for you.

Q365 **Tim Loughton:** Is it a single figure, a double figure, a triple figure or more?

Steve Smart: I don't have the figure, I am afraid.

Q366 **Tim Loughton:** That is slightly disappointing. This is the sort of thing that this Committee is very interested in. At previous hearings, the issue specifically came up of how it is possible to operate these bogus bank accounts, which are absolutely the bread and butter of these fraudsters, who use them to extract money from unsuspecting victims. One major control over that must be the way that firms that make a business out of handling people's money responsibly follow the regulations and procedures. The person who makes sure they are following the regulations and procedures is the Financial Conduct Authority. You have not been able to tell us, even roughly, how many accounts have been responsible for this sort of fraudulent activity or how many firms have lost their licence because they do not properly have a handle on this fraudulent activity. Even though there has been some drop in fraud activity, this activity still amounts to millions of crimes in the biggest part of crime in this country. So your role is crucial in all of this—and you have prosecuted 10 people.

Steve Smart: Last year. I said at the outset that we are not a volume prosecutor or investigator in that space. That is criminal prosecutions. There is work going on, obviously, in the regulatory space.

Q367 **Tim Loughton:** You have 190 live investigations at the moment.

Steve Smart: Live operations, yes.

Q368 **Tim Loughton:** You are funded by your member firms, aren't you?

Steve Smart: Yes.

Q369 **Tim Loughton:** How much revenue does that bring in?

Steve Smart: I think that the budget for the organisation is about £780 million.

Q370 **Tim Loughton:** How many people do you employ for £780 million?

Steve Smart: Roughly 5,000.

Q371 **Tim Loughton:** How many of those are enforcement agents?

Steve Smart: Our enforcement function is about 600 people.

Q372 **Tim Loughton:** Do you have enough enforcement agents?

Steve Smart: Given that we are not only there to enforce, and given the size of the organisation, yes.

Q373 **Tim Loughton:** Where do your fines go?

Steve Smart: Our fines will go back to the Home Office or back to the Government—sorry, back to Treasury; will go back to the Home Office—after we have taken out the costs of enforcement from our fines.

Q374 **Tim Loughton:** It is 24 years since I was in the City. The forerunner of the FCA was set up in the 1980s, and I thought that all the fines at that stage went to—I can't remember what the original FCA was called.

Steve Smart: The FSA.

Tim Loughton: The FSA, correct. It took all the fines.

Steve Smart: I don't know. I wasn't in the organisation then.

Q375 **Tim Loughton:** I suppose those fines were used to offset the level of fees that firms had to pay. Do your fees move up and down accordingly?

Steve Smart: Our fees are set each year. The amount that individual firms pay can be impacted by the amount of fines that we receive. We take out our costs of enforcement and then there is a rebate to the firms that have not been involved in wrongdoing.

Q376 **Tim Loughton:** How many times have your subscription levels gone down in the last few years?

Steve Smart: I don't think our subscription levels have gone down in the last few years but, again, I don't have that information to hand.

Q377 **Tim Loughton:** If you are doing a good job on fining your firms, is it because the costs of running your organisation have got higher that you are not redistributing to your member firms as you were set up to do?

Steve Smart: I am not sure I quite follow the question there.

Tim Loughton: You just said that your subscription levels have not been reduced because you have not been able to redistribute fine levels to those firms after you have taken your cut before the money goes to the Home Office.

Steve Smart: The Treasury.

Tim Loughton: It is now the Treasury? I think you said the Home Office.

Steve Smart: Yes, I did. I think I corrected myself.

Tim Loughton: The point I am trying to make is, do you think you should be raising more fines, in which case there will be more money to go back to your member firms, or would those fines just be gobbled up because of the cost of running your organisation?

Steve Smart: I think we should be focusing on what we set out in our strategy, which is to prevent and reduce economic crime, and we should be looking to do that the best way we can. There is the supervisory activity that we take with firms on systems and controls, and the work we

do with them in the technology space. I came in on the end of the previous panel, where I think you were asking who takes advantage of technology the quickest, the criminal or the enforcement side. I want to get us into a space where we are working with firms and they are able to take advantage of the opportunities that new technology and artificial intelligence produce, because the criminals are very agile at doing that.

Last month, we released a set of synthetic data that the firms can use in what we call our digital sandbox, which is effectively an area you can come into to trial your systems and controls to see whether they will help you spot things like money from APP fraud coming in. We are working with firms on how they identify individuals behaving in a way that they would not expect them to be behaving, through using social—

Q378 **Tim Loughton:** I understand. I need to let other people ask their questions, but it would be helpful if we could have some more figures about the prevalence. I just don't understand: you keep telling us that you are not a volume organisation, but this is a volume crime, which appears to be going up in terms of the use of fraudulent bank accounts. Your organisation is there to make sure that that is not happening, but it clearly is, so we need those figures.

Chair: You will provide those figures for us.

Steve Smart: Yes, we will provide those figures.

Chair: Thank you.

Q379 **Alison Thewliss:** Mr Las, what is HMRC's enforcement strategy for investigating tax fraud, and what impact does tax fraud have on the public?

Richard Las: Overall, we have a strategy that encompasses a whole range of our powers. It is based on three principles: prevent, promote and respond. We are trying to prevent fraud by making sure we harden our systems—bearing in mind that we are talking about tax fraud principally—so we have a good degree of control over those systems. We try to promote good compliance by engaging with taxpayers and our stakeholders to make sure they are aware of what the rules are. We then respond where we need to, which is essentially our interventions.

It is important to understand as well that HMRC is a very large organisation, and essentially we conduct about 300,000 civil interventions every year. They are not all into fraud; they are into areas of non-compliance. Last year, that work generated £28 billion roughly. It is a very significant activity. My part of the organisation, which is the Fraud Investigation Service, focuses specifically on fraud and the more serious kind of fraud.

Q380 **Alison Thewliss:** How many people do you have in your department working on tax fraud? How many prosecutions does that lead to?

Richard Las: We have around 5,000 people in total in the Fraud Investigation Service. Broadly speaking, about 1,500 of them are criminal justice-trained, so they will be working on criminal investigations. A similar number might be doing civil investigations of all sorts. Then we have other responsibilities—for example, risk supervisor for money service bureaux. We do recovery work and things like that. Broadly speaking, those are the numbers.

Last year, we opened about 12,000 civil investigations, and we opened about 400 additional criminal investigations. In my current portfolio, I have about 1,000 criminal investigations—individuals being investigated who are within the system and potentially going towards trial.

Q381 **Alison Thewliss:** As an organisation, are you more interested in recovery of moneys that have not been paid or in prosecuting people for not paying?

Richard Las: It is a bit of everything. Ultimately, HMRC's area is to collect the correct amount of tax, so that is what we are trying to do. We try to do that in the most effective and efficient way. That is why, in a lot of our cases, we will be dealing with that through a civil investigation. A civil investigation would ideally lead to all the tax that has not been paid being identified and recovered. We can levy penalties of up to 200% of that tax, and we can charge interest on top of that. In terms of a resolution for HMRC and the Government, that is a good deal.

On the prosecution side, we tend to be looking at cases where there is more serious behaviour, where there is a high level of harm in terms of the amount of tax that has been taken, where there is a particularly systemic and sustained attack on the tax system or where it is novel. Those are the sorts of areas where we would be mainly going to a criminal investigation, or where we believe that a civil investigation just will not work. That is potentially, if we are looking at organised crime, the sorts of areas where it is unlikely that sending a bill will result in a payment.

Q382 **Alison Thewliss:** They are not that interested in paying up. Lots of things were said about fraud during covid. Where does that currently stand with HMRC? How much of the fraud during covid have you been able to chase down? I say that because, to give an example, I had a company in my constituency that claimed furlough money for employees but set up a series of payroll companies, and the employees never saw that money. I am curious about cases like, where company structures have been quite clearly set up and abused to avoid paying employees what they were due. Where do those cases stand?

Richard Las: We are still looking at covid cases. We did a lot of work during the pandemic on trying to act quickly on cases to ensure that we could prevent fraud from happening and also create an immediate deterrence. In terms of our final estimate of error and fraud—so it includes error—across all the covid schemes that we ran, the most likely

midpoint is about 5%, which corresponds to about £5 billion in total. We did compliance activity all the way through the pandemic and continue to do so. That compliance activity has protected about £1.6 billion of payments that would otherwise have been made fraudulently or in error.

Q383 **Alison Thewliss:** What was the 5% you said? I didn't quite catch what you said.

Richard Las: The 5% is our level for what we believe the error and fraud was from all the covid schemes that HMRC ran.

Q384 **Alison Thewliss:** I will leave that for the moment. Separately, can you tell me how HMRC exchanges information on suspected fraud cases involving terrorist financing?

Richard Las: We exchange information across a lot of areas. We one of the biggest holders of information in the country without doubt. Principally, we do three levels of exchange, and this might cover some of the other points that come up.

We routinely exchange information with other agencies about fraud or that will help tackle fraud, for example. Typically, that might be information about income that we share with the Department for Work and Pensions, just to bring that to life.

Equally, if we identify intelligence or information that is relevant to another agency, whether that is fraud or terrorist financing, we will direct it to the other agencies. That is where we push information out, so that probably captures your question. We will identify that, whether in the course of our investigations into money movements or as part of our work on sanctions and prohibitions. We refer that to the relevant agency, depending on what is happening specifically.

Finally, we respond to requests from other agencies. That is a pull from us, and we will provide that information.

Q385 **Alison Thewliss:** What are the highest areas by volume of fraud that come to HMRC?

Richard Las: We cover a whole range of tax frauds. Our current estimate for losses to fraud and organised criminal attack is about £9 billion between the two. It is split broadly equally between the two. The fraud estimate is spread between a lot of players. Some elements of that are organised fraud, which are very large, typically involving supply chains where tax is taken out of the supply chains—it could be for labour or for anything like that. Equally, we do a lot of work on organised crime, where it could be to do with tobacco smuggling or alcohol fraud as well. We have sub-estimates for all of those that are published each year, but generally our approach will be to target the areas of the highest risk where we believe we will have the best chance of having an impact, and we manage it in that way.

Q386 **Alison Thewliss:** Do you feel you have sufficient staff resources to tackle this? Fraudsters are quite adept at trying to get around things. Are you able to hire and retain people with the level of expertise that you need?

Richard Las: On overall levels of resource, every year we will get a settlement based on a number of factors, but there might also be a specific fiscal event that gives us resources to tackle a specific problem—that tackles new risks or growing risks, where we would do that. Equally, our aim is to try to maintain the tax gap at about its current level or to push down a bit. There is where we are operating it, and I think we have enough resources to do that.

On the question about skills and capabilities, we definitely have to grow different capabilities as the fraud changes. Fraud has become more technical. We have heard some of the issues with online fraud. We deal with vast amounts of digital information, and we need people who understand that and who can manage it, deal with it and present it. We have to change the skillsets of our investigators. If I think back to what it was like 20 years ago, I might have one phone that I have to look at in an investigation. Now I could have four phones plus computers as well. It is a much more complex issue.

Q387 **Alison Thewliss:** Mr Smart, I recall from my time on the Treasury Committee and from some of the evidence that we have heard in this Committee that people can fall victim to investment fraud not just once but multiple times. I recall from my time on Treasury that some of those investment frauds were considered to be outside the FCA perimeter and, therefore, not your problem and not something you would necessarily have recourse to look at. Where does that currently sit?

Steve Smart: We take action on firms outside the perimeter who are engaging in investment fraud if they are operating as if they were within the perimeter. On a daily basis, we scrub 100,000 websites in the financial services sector for those sort of adverts. If we identify firms that are effectively pretending to be regulated and looking to engage in investment activity but that are not regulated, we will look to prosecute them. The majority of the prosecutions that I was talking about previously revolve around firms that are outside the perimeter.

Q388 **Alison Thewliss:** It is a relatively small number that get to that point.

Steve Smart: It is a relatively small number, yes, which is why I think it is the prevent space where we can really have the impact. Twelve months ago, working with the big tech companies across the board, we got them into a position where, for paid-for adverts, they now voluntarily agree to check companies against the FCA watchlist or against the FCA regulated list to ensure that they are regulated. If they are not regulated, they will remove those adverts. Unlawful paid-for adverts have dropped by 100% over the last 12 months.

Q389 **Alison Thewliss:** There is still a significant loophole there for the non-

paid-for element of that. On Instagram and TikTok there are all these people advertising financial advice or investments and things like that, so the non-paid-for part is quite significant.

Steve Smart: Yes, it is, and that is the big issue now. As the Online Safety Act comes into force, and the voluntary charter with the tech companies, we want them to be much more proactive on the self-generated adverts—the things that are on social media. There is a lot of work still to do in that space.

Q390 **Alison Thewliss:** Is that legislation making it voluntary rather than mandatory a gap—a missed opportunity?

Steve Smart: I think that the legislation, as it comes into force, will help with that and that the voluntary agreement, if followed through, will have a big impact. Everybody talks about fraud needing a team-based approach, and big tech absolutely needs to be part of that team. We all need to keep focused and pushing on that.

Q391 **Alison Thewliss:** Yes, because the scale of this content is quite incredible. It is impossible for you to look at, and that is impossible for the police and law enforcement to do. Surely, the companies ought to have the responsibility.

Steve Smart: They absolutely have to take some responsibility. The scale—I think this whole conversation started with the Chair's question about the scale—is so big that you cannot arrest and prosecute your way out of it. It is about how you find the best way to prevent it, and we have a privileged position working with the firms in the financial sector to help put protections in place. It is about educating the consumers and members of the public on what to look out for. We run a number of campaigns, such as ScamSmart and InvestSmart. ScamSmart has been running since 2014, with over 2 million hits on our website. The more we can educate people on what to look out for, the better we will be at trying to stop some of this.

Q392 **Alison Thewliss:** Do company structures make it more difficult to track down the people responsible for doing these things?

Steve Smart: Yes, I think they do. The Companies House reform and the work that is going on there will make a big difference and help us a lot. There are lots of things that make fraud difficult. The technology brings lots of opportunities. You can commit a fraud in the UK now from anywhere in the world. You do not have to be in the jurisdiction to commit a fraud. There is so much of it operating online. The last figures that came out suggested that about 80% of fraud is cyber-enabled. It comes online from anywhere in the world. That also causes lots of jurisdictional issues for you when you are trying to get to the individuals doing it and to prosecute them.

Q393 **Alison Thewliss:** I appreciate that it is early days, but has the Economic Crime and Corporate Transparency Act had an effect yet on the failure to

prevent fraud?

Steve Smart: It is early days. It is a power that I think the SFO will be making quite a lot of use of, and it will be there as something for us to use. We have quite a lot of powers already in some of the areas, but we need look at this all holistically and bring everybody's focus to bear on it.

From my perspective, one of the big positives at the moment is that there is a real focus on fraud from the Government down. We need to ensure that that stays there and that we keep that priority on, it if we are going to make the progress we all want to make.

Andrew Penhale: The failure to prevent fraud offence will only come into effect once Home Office guidance is provided for businesses, and that is in the process of development and consultation at the moment.

Q394 **Carolyn Harris:** Mr Penhale, you said in response to a question from my colleague earlier that you thought the police had other priorities and that maybe fraud was not at the top of those priorities. We have done quite an in-depth inquiry into policing priorities, and fraud came out as one they really did feel was important for them. I don't think any police force will admit this publicly, but do you think that there is a sense, privately, that the CPS's reluctance to prosecute is not a motivation for the police to pursue prosecutions?

Andrew Penhale: Do you mean that that is put forward as an explanation for not investigating fraud—that the CPS—

Carolyn Harris: No. I just think it is quite demoralising when you investigate any case. With rape, for example, a huge number of rape cases do not get to court because the CPS are not willing to prosecute. Do you think that that could be demotivating for the police?

Andrew Penhale: I do not think it is in relation to fraud. I am the economic crime lead, so I can only talk about the fraud and economic crime area. We charge 75% of the cases that come to us, so we take forward as prosecutions three quarters of the cases that are referred. It is fair to say that the numbers are low, and that means that there will always be an issue with capability and capacity and so on within our system, as well as in policing.

We are working hard to try to upskill some of our lawyers to make sure they understand how to operate on complex frauds, how to prosecute complex frauds and how to advise investigators during an investigation. We will often support investigators at a very early stage when they are investigating fraud. So we have an interest in that as well, and we give them early advice to produce a successful prosecution.

We work very closely with policing, as well as with other agencies. I do not think we are in conflict with them at all in that respect. I am really pleased that fraud is more of a priority than it has been in the past. The reality is, of course, that there are all sorts of pressures and demands on

policing, but it is great that there is now an initiative to generate 400 extra fraud investigators, and we really welcome that. Certainly from the CPS perspective, we will not be turning that work away; we will be working with policing to generate successful prosecutions wherever we can.

Q395 **Carolyn Harris:** We have heard a lot of evidence from the police on fraud, and from what they tell us they are quite good at investigating fraud. They are training people and recruiting people specifically. They acknowledge that crime has changed and that the kinds of crime being committed will more often be fraud or cyber-crimes. What do they need to do to allow you to make more prosecutions?

Andrew Penhale: Essentially, to generate more, more need to be brought to us. The quality of investigations is often very good. It was interesting hearing from the City of London police this morning. The force has real expertise in this area, and it is great that they are supporting policing to develop more expertise across the country.

In a similar way, we build that expertise within the CPS. I lead a team that is very specialist in this area. We have capability around asset recovery, so people who are specialists in asset recovery. We have specialists in international work, including people who operate all over the world, who work with a range of agencies as well as our own. We can tap into those resources to help our prosecutors, but also to help the investigators during an investigation.

We have a model that can really assist investigators, but we are not in conflict with them. We all have the desire to prosecute and bring criminals to justice, and hopefully to give victims some recompense.

Carolyn Harris: I sincerely hope that that is the case. We have heard a lot from Mr Las about the Inland Revenue and the HMRC issue, but I worry about the Mrs Joneses and Mr Davises who do not have a huge amount of money to lose and who are losing money continually because they are very vulnerable to the kinds of crime that we are talking about. That is it from me, Chair. Thank you.

Q396 **Chair:** Can I just ask one last question. We have talked a little about tech companies. What is your relationship like with the tech companies? Do you think they are pulling their weight and doing their bit? Do you want to start, Mr Penhale?

Andrew Penhale: I am really pleased that the online crime Bill requires them to do more. They need to be in a position to share data more freely with law enforcement and also to be proactive in blocking and stopping fraudsters from operating. We really welcome that.

In terms of supporting us when we conduct prosecutions, we do work very closely with the large tech companies in securing evidence from overseas and elsewhere. We see them working closely with us when we have to.

Q397 **Chair:** You are saying that that is quite positive. That is often not the impression we get when we talk about the tech companies.

Andrew Penhale: There is always more that can be done. I have absolutely no doubt there is more they can do in identifying fraud and stopping it at source, but in terms of us working with them to secure successful prosecution, we generally find that they co-operate with us.

Richard Las: I am happy to comment a little bit on that one. To put it into a bit of context, when we talked earlier about the accounts and the problems there, a lot of that is about people's credentials being farmed by organised crime groups. In 2015, HMRC was the third most phished brand globally—not surprisingly, because I guess we are seen as a trusted brand. We are now well outside of the top 100 of abused brands—that is not to say that there are not still a lot of emails purporting to be HMRC—but how have we got to that position? Part of that has been about the work we do with all the tech companies in trying to identify bogus emails and to take down sites that are selling fraud schemes or targeting individuals. There is always more that can be done, but we have made a lot of progress there in practical terms.

Steve Smart: We covered it a bit earlier. We did some good work with the tech companies on paid-for adverts, but there is a lot to do with self-generated. We need companies to be in a more proactive space and looking to identify these things and take them down.

Chair: Thank you very much indeed for your evidence this morning. That has been very helpful. Thank you. That concludes our session.