HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: Progress combatting fraud, HC 40

Thursday 1 December 2022

Ordered by the House of Commons to be published on 1 December 2022.

Watch the meeting

Members present: Dame Meg Hillier (Chair); Olivia Blake; Sir Geoffrey CliftonBrown; Mr Jonathan Djanogly; Peter Grant; Sarah Olney; Nick Smith.

Justice Committee Member present: Sir Robert Neill, Chair.

Gareth Davies, Comptroller and Auditor General, National Audit Office, and Lewis Holden, Head of Accountability and Governance, HM Treasury, were in attendance.

Questions 1 - 124

Witnesses

I: Matthew Rycroft CBE, Permanent Secretary, Home Office; Duncan Tessier, Director, Economic Crime, Home Office; Graeme Biggar CBE, Director General, National Crime Agency; Pete O'Doherty, Assistant Commissioner, City of London Police.

Report by the Comptroller and Auditor General

Progress combatting fraud (HC 654)

Examination of witnesses

Witnesses: Matthew Rycroft CBE, Duncan Tessier, Graeme Biggar and Pete O’Doherty.

Q1 **Chair:** Welcome to the Public Accounts Committee on Thursday 1 December 2022. Today we are looking at the knotty issue of how Government, and different agencies and organisations, combat fraud. Fraud against individuals and businesses is a growing issue, which this Committee last looked at five years ago. In the year to June 2022, fraud represented a shocking 41% of all crimes committed against individuals. When we were preparing for this session, it sometimes felt like it was everybody’s problem but no one’s priority. We raised concerns back in 2017, and the problem has got worse since then, not better.

We have questions today of various parts of Government that are working to tackle fraud about whether the Home Office is leading effective crossGovernment work on the issue, and whether the different agencies are playing their role. I want to thank those who have submitted evidence on this very important topic as well.

I would like to welcome our witnesses. We have Matthew Rycroft, who is the Permanent Secretary at the Home Office. He is joined by Duncan Tessier, the Director of Economic Crime at the Home Office. Then we have Graeme Biggar, the Director General of the National Crime Agency, and Pete O’Doherty, who is Assistant Commissioner for the City of London Police. The City of London Police is the police force in England that deals with fraud and is the centre for all the fraud expertise, which then rolls out to other police forces. This is an issue in itself that we want to talk about today.

Before we go into the main session, I just wanted to ask you, Permanent Secretary, about the appalling situation at Manston. We have gone through the issue of overcrowding. First of all, have you yet had any legal challenges about the overcrowding and the impact on individuals at Manston?

Matthew Rycroft: Yes. At the last count, we have had five pre-action protocols in relation to Manston in total.

Q2 **Chair:** Do they relate to individuals?

Matthew Rycroft: Each of them is slightly different from the other, but they relate to the conditions and the length of stay in Manston.

Q3 **Chair:** There does not seem to be a ministerial direction that we have seen about this. At any point did you advise Ministers that there might be an issue about breaking the law?

Matthew Rycroft: Yes. The Home Secretary and I gave full evidence to the Home Affairs Committee just last week on this very issue. As I said to them, there was a steady stream of legal advice to this Home Secretary and to her predecessors.

Q4 **Chair:** Okay, and at no point did you feel any need to ask for a ministerial direction about the use of Manston.

Matthew Rycroft: No, because we gave the advice to Ministers and we had, and continue to have, a clear plan to reduce the amount of time that each person is in Manston back to lawful levels.

Q5 **Chair:** But when you introduced Manston, there must have been a plan before it got overcrowded about what would happen if it did get overcrowded. It did not seem to work, if so.

Matthew Rycroft: The first thing to say is that, of course, the facility at Manston is significantly better than what we were using before. Although it has been in the news for all the wrong reasons, it has a much better screening capability than we previously had when we had to do everything right on the seashore at Western Jet Foil in Dover. It is a significantly better facility. We have had a lot of co-operation from the military; it is a former military site. We have expanded the capacity of Manston. Of course, it continues to be an initial holding facility where our aim is to do the initial screening of every individual within 24 hours. Unless there are exceptional circumstances to keep them there beyond that, or unless we extend that 24-hour period, which is conceivable, then people should be moving on to the next accommodation after that.

Q6 **Chair:** In the past, we have also looked at the issue of putting people into hotels in different areas. Two years ago, we recommended to your Department that you work better with councils and with MPs. You accepted our recommendation in January 2021; we made that recommendation in November—almost exactly two years ago. Yet we have seen exactly the same situation, where people have been housed at haste into city centres and areas without notification of the local authority or the proper local support that is necessary to support vulnerable people, often alone, in a strange country. Why did you accept our recommendation and then completely fail to deliver?

Matthew Rycroft: We continue to accept the recommendations, and we continue to deliver. As the Home Secretary told the Home Affairs Committee last week, Minister Jenrick, the Immigration Minister, set out to all MPs a new system of engagement in relation to hotels.

Q7 **Chair:** That is exactly my point. I was in the House when he talked about this new system of engagement like it was some revelatory thing, yet two years earlier this Committee had said, "You are not engaging properly." We had one of the biggest write-ins I have had from MPs, who we canvassed for views on the work we are doing, to tell us that they had been

completely bounced and blindsided. For example, they said they had read in the local newspaper first that this was happening and, when they checked, their local authority had had no contact either. We called it out then, we were told it was going to change, yet it is being announced as though it is an exciting new initiative by the Minister. I am not blaming the Minister for that, but it did not happen, did it?

Matthew Rycroft: I do not think he, or anyone else, thought that it was that exciting. It was part of continual improvements, learning the lessons from previous engagement with MPs and understanding the importance of engaging with local partners, whether that is the local authorities or the local MP. This is in relation not just to hotels, but to all types of accommodation. Sometimes we put our hand up and say that we were unable to meet the standards that we would hope to in terms of preengagement before moving people, because of the significant numbers on some occasions. That is why we have put in place an improved procedure, just to make sure that that happens every time. Since then, subject to any of you giving additional feedback, there has been a bit of an improvement. It continues to be a work in progress, and we will continue to listen to you and any other MPs.

Q8 **Chair:** For this Committee, we made a recommendation; your Department accepted that recommendation and then did not deliver on that recommendation. There is a difference between saying you agree with the Committee and accepting it, and then actually doing it. It makes us consider whether we should have a further follow-up on all these Treasury minutes, because saying you are doing it, and then not doing it, is not really playing the game by the rules.

Matthew Rycroft: Just to be clear, we did accept that recommendation and we have been acting on it. What I have just put my hand up and said is that we have not always successfully met the level of engagement before migrants are moved into individual hotels, or other accommodation, in any individual MP's constituency. That is what we are seeking to do. We are improving that engagement in very difficult circumstances, and we will carry on listening to feedback, as we have done in the run-up to, and subsequent to, Minister Jenrick's letter. If there are further improvements to the system that this Committee, or anyone else, would like to suggest, we will be very keen to hear them.

Q9 **Nick Smith:** Mr Rycroft, thank you for that answer. What does the data say? You say you have met the recommendation of the Committee. How often have you told MPs or local authorities about these movements, and how often have you failed to do that? Can you give us your record in the last year, please?

Matthew Rycroft: I will happily write to the Committee with that data. It is fair to say that there is a lot of noise about this. We totally understand why, but the fact is that we have had record numbers of migrants crossing the channel this year. Any of them who would otherwise be destitute, we have a statutory obligation to accommodate. That accommodation has to be in someone's constituency, and that is why we have this engagement.

I am very happy to write with the details. I think there is a lot of noise about the minority of cases where the engagement has not gone as well as it should, but I will happily set out the proportions.

Q10 **Nick Smith:** We have taken your acceptance of our recommendation in good faith and we expect it to happen reasonably well after that. Please get back to us with the detail to see whether you are doing what you say you will do.

Matthew Rycroft: Absolutely, and that goes for all the PAC's recommendations that we accept. We have systems in place to track them. I personally am very interested in that. That is why I write so many Treasury minutes and so many updates on some issues, like our favourite: IT programmes for policing. I write quarterly to you as a way of keeping that flow of information going. If there are other issues that I should do that on as well, I am very happy to do so.

Q11 **Chair:** The recent issue of the outbreak of diphtheria and the sad death of an individual who passed through Manston raises really serious issues about public health problems. Given you have had the experience of covid and the pandemic, what went wrong that this was not picked up and public health officials were not alerted about people being dispersed around the country with diphtheria?

Matthew Rycroft: The first thing to say is that my heart goes out to the family of the individual involved. Without straying into the territory of an inquest or any other inquiry, it is fair to say that he did not have any symptoms of diphtheria at the time that he was in Manston. We have set up a full vaccination programme for diphtheria since 15 November for people coming into Manston. We remain in very close contact with our colleagues from Public Health England and other health authorities. At the Home Secretary's direction, we have improved the medical facilities available in Manston, and we will continue to listen and act on any advice from our public health colleagues.

Q12 **Chair:** Regardless, diphtheria was an issue that was being talked about before the case was diagnosed. Public health officials are on record saying that they did not have a good engagement with you as people were dispersed. Knowing that you had people crammed, in large numbers, into a facility not designed for those numbers, there was always going to be a risk of this. Surely you had some planning for this.

Matthew Rycroft: Absolutely, and, as on so many other issues, we have to balance the risks that we are dealing with. The safest thing to do, if there were any possibility of diphtheria, would be to keep everyone in Manston in Manston. That would add to the problems that you alluded to at the very beginning.

Q13 **Chair:** Sorry, you are saying the safest thing would have been to keep people in Manston. An overcrowded Manston, with someone with diphtheria, would— ***Matthew Rycroft:*** Exactly.

Chair: That would maybe be safer for people outside Manston, but not for people in Manston.

Matthew Rycroft: We have to balance all these risks. This is why we listened to Public Health England, and why on this occasion we went ahead with dispersing people who, as it turned out subsequently, did have diphtheria. We have been learning from that and engaging with our Public Health England colleagues.

Q14 **Chair:** Did it occur to anyone that there was a case of diphtheria and some of those people might have diphtheria when you were dispersing them to other parts of the country?

Matthew Rycroft: Yes.

Q15 **Chair:** Did you inform the public health officials in each area that you were sending people to?

Matthew Rycroft: I will have to check that.

Chair: Could you write to us on that, please? The Home Office is not an island in its own right. This is having a big effect on local communities and, of course, the poor individuals concerned, who did not expect this. They have had lots of challenges, but getting diphtheria is a huge issue.

I will pause there on that for now—I know our sister Committee is pursuing this vigorously—and turn to Sir Geoffrey Clifton-Brown on a slightly different issue.

Q16 **Sir Geoffrey Clifton-Brown:** Morning, Permanent Secretary. Can you just give us an update on Ukrainian visas, the trend, and whether you are getting enough sponsors under the sponsorship scheme?

Matthew Rycroft: We continue to be bowled over by the generosity of the British people in coming forward to offer their spare rooms or spare accommodation for Ukrainians who have fled Putin's illegal invasion. It has come in waves, largely depending on events in Ukraine. My view is that, in a way, it is better if people stay in or very close to their home country, so we do not celebrate when extra people want to come here, but we are seeking to keep the scheme going for as long as it is needed. Of course, there is a lot of planning going on now in relation to different scenarios for the winter, which is fast upon us.

I will happily write to the Committee with the latest statistics, but we have systems in place. We continue to appeal to British people who want to offer accommodation and become a sponsor to do so, or, if they are already, to continue to do so. We are working with our colleagues in the Department for Levelling Up, Housing and Communities, and will continue to ensure that those people get some financial reward for their generosity.

Q17 **Sir Geoffrey Clifton-Brown:** Thank you. It is just that, for many, the sixmonth period is now coming up. I am about to have a meeting with some of those. Is there a good substitute six-month hosting scheme available, so that if these people get to the six months and they do not want them to stay—I can understand that—there are enough people out there willing to take over?

Matthew Rycroft: We are working very closely with our colleagues in DLUHC, and I will write to you with the numbers.

Q18 **Olivia Blake:** Just to go back to the Chair's questions, are you just vaccinating or are you also screening and testing people who are coming into the facilities at Manston?

Matthew Rycroft: For diphtheria?

Olivia Blake: For diphtheria and other communicable diseases.

Matthew Rycroft: I had better check that and write to you.

Q19 **Olivia Blake:** Thank you. Surely isolation in a medical facility would make more sense than holding people in a space where we know there have been quite drastic public health failings.

Matthew Rycroft: The issue is who. If one is asymptomatic, then—

Olivia Blake: But that is why screening would be helpful, isn't it?

Matthew Rycroft: Yes, absolutely. I will get back to you on the screening point.

Q20 **Chair:** We look forward to a note on that.

We now move into our main session. First of all, I want to ask about the fraud strategy that you announced seven months ago. When is it going to be published?

Matthew Rycroft: As early as possible in the new year.

Q21 **Chair:** In civil service terms, does that mean by Easter, or do you think it might be January? Do you have a window of time?

Matthew Rycroft: I really hope that it will be very close to the new year.

Q22 **Chair:** What are you hoping that it will achieve, and by when? We last looked at this five years ago, as I said in the introduction, and things have got worse since then. In broad terms, what are you hoping to achieve?

Matthew Rycroft: First of all, we agree that the scale of the challenge has got bigger since 2017. We welcome the National Audit Office Report and its very clear recommendations, which we accept.

The record of achievement in response to this threat, which is growing, is not negligible. Since 2017, there have been some successes. There has been a significant injection of funding into policing, to the tune of £400 million over this spending review period, to enhance law enforcement and intelligence capabilities in response to fraud. But we absolutely accept that we need to go further and faster. What we really need is a co-ordinated, holistic strategy, bringing together Government, law enforcement and industry, using the NAO framework for how to write and deliver a really effective strategy that is based on outcomes. That is what you will see as early as possible in the new year.

Q23 **Chair:** That explains, really, why we are doing the session, because that co-ordinated holistic strategy is what we all want to see. Before I pass over to Sir Bob Neill, who chairs our sister Committee, the Justice Committee— I should have introduced him as our guest—are you expecting that the strategy will also include requirements for legislation?

Matthew Rycroft: There has already been some legislation and there continues to be some before the House, including the Online Safety Bill. I do not think that will be the main focus of the strategy, but the strategy is still with Ministers and it has not been through its full consultation. We have been talking to a lot of people about it. We have been drawing on the Justice Committee's report—for which many thanks, Sir Bob—as well as the NAO Report and views from industry. It is really important that we have an incredibly close relationship with the financial services sector, the telecoms sector, the tech sector and many others. We are listening to those and integrating.

Q24 **Chair:** At the moment, either you cannot tell us or you are not expecting further legislation at this point, other than what is going through.

Matthew Rycroft: No, not in addition to the legislation that has already been announced, I am afraid.

Duncan Tessier: Is there a specific proposal that you had in mind?

Q25 **Chair:** One of the issues that I was going to touch on later is around cryptocurrency. For example, banks are required to put out lots of adverts about anti-fraud measures on the same social media that is often interspersed with things such as adverts for cryptocurrency, which quite young people will see, in all sorts of interesting places, with no real health warnings. You have this juxtaposition of trying to stop it on a social media platform, cheek by jowl with someone telling them to do something that is not necessarily safe. There is nothing on the social media platforms to stop that.

Duncan Tessier: The Online Safety Bill is the right first place to go. There is also the online advertising programme. Both are led by DCMS.

Q26 **Chair:** You think those will nail it.

Duncan Tessier: Yes, I think they are going to make a really big difference.

Chair: We may pick up on that as we go through. First of all, welcome, Sir Bob.

Q27 **Sir Robert Neill:** Thank you very much, Dame Meg. I am very grateful for the opportunity to be here. Gentlemen, perhaps I could just follow up on a couple of issues that touch upon our report. A fraud strategy has been talked about for a long time; there has been a national fraud plan before that. We have not yet seen it. Who has ownership of this strategy? Who within Government is going to own it?

Matthew Rycroft: The Home Office owns the overall strategy for combating fraud. The Home Secretary and the Chancellor jointly chair the top strategic level board. At ministerial level, the Security Minister, Tom Tugendhat, is the lead Minister for tackling fraud. We work very closely with our operational partners, hence the appearance of my colleagues on this panel. The National Crime Agency leads and co-ordinates the operational response. The actual response in so many investigations, including the very successful one by the Met last week, is led by territorial policing, co-ordinated by colleagues from City of London Police.

Q28 **Sir Robert Neill:** Do you perhaps think that there needs to be stronger governance and ownership at both political and official level? It is still very diverse, isn't it?

Matthew Rycroft: We have acted on your Committee's recommendation to strengthen and streamline the governance already. It is diverse in the sense that this is a very complex landscape and, as the National Audit Office Report and your own set out, we need join-up across that landscape. There are an awful lot of people who have a role to play under that system leadership that the Home Office seeks to provide. We need join-up across the criminal justice system, working very closely with our colleagues in the Ministry of Justice, the Crown Prosecution Service and others, as you would expect, but also with colleagues in financial services and other industry sectors.

Q29 **Sir Robert Neill:** How many officials do you have in the unit in Home Office that is dedicated to tackling fraud?

Matthew Rycroft: Mr Tessier is the director leading that unit.

Sir Robert Neill: How much resource do you have, Mr Tessier?

Duncan Tessier: There are about 110 officials in my economic crime directorate, and we have a fraud policy unit that has about 20.

Q30 **Sir Robert Neill:** One thing that struck both Committees, which was in the National Audit Office and the Justice Committee's reports, was that fraud is about 40%, give or take, of recorded crime—most people would accept that that is probably an underestimate because of the very low levels of reporting—but it has only about 1% of police manpower and about 2% of dedicated police resources. What are the plans to increase the amount of resourcing that is dedicated to fraud within the policing system?
Perhaps Mr O'Doherty can help on this.

Matthew Rycroft: We can confirm that it is now 41% of overall crime. You are right that it has about 1% of policing resource, so that definitely needs to increase. The total amount going to policing is increasing, of course, through the 20,000 police uplift programme and other Government decisions, to ensure that policing is getting what it needs in terms of resource. There is the £400 million over these three years specifically for fraud, which I have already mentioned. Mr O'Doherty can perhaps speak in more detail about where that is going.

Pete O'Doherty: The investment we are getting through the spending review is going to achieve new technology for Action Fraud and the NFIB, making this service more user-friendly for victims, more available, more accessible and much more efficient.

We are building 10 proactive fraud investigation teams around the UK, working with local and regional policing, using intelligence more proactively to try to identify and disrupt fraudsters before it is too late.

Lots of investment is going into improving victim care and support services. I am really excited about the impact that is going to have over the next two to three years.

Q31 **Sir Robert Neill:** One thing that concerns us is how much expertise there is outside the City of London. I do not mean it pejoratively, but provincially, some would say that some of the county and other police forces outside London simply do not have the resource that exists within the City force. What is being done to strengthen capacity in forces across the country?

Pete O'Doherty: There are two bits here. First of all, it is indeed correct that given the ever-increasing complexity of fraud, which is internationally driven, and the use of technology—we spoke about cryptocurrencies earlier—we are doing loads of work with our Economic and Cyber Crime Academy and the College of Policing to improve the level of specialist training given to police officers investigating fraud.

Secondly, the new people we will be recruiting into those proactive teams will be provided specialist training. Indeed, that syllabus and programme of training has already been designed by the City of London Police.

Lastly, we have a big issue around attrition. As you can imagine, the specialist people we need are very attractive to the outside world. In partnership with the National Economic Crime Centre and the NCA, we are developing a people strategy, working with industry and volunteer programmes to help improve the way we attract, recruit, retain and indeed develop our people.

Q32 **Sir Robert Neill:** The issue you raise, Mr O'Doherty, about a more victimfriendly approach is important in terms of what replaces Action Fraud, is it not? One of the real concerns we have is that Action Fraud is nicknamed "Inaction Fraud"; it is frankly seen as a black hole by many victims. This is why, more often than not, they do not bother to use it.

Our report expressed a concern that the replacement for Action Fraud would concentrate on data collection and capture, and processes being improved, but, as far as we can see so far, did not have anything about responding more effectively to victims, keeping them better informed and making it easier for them to report. What is going to be done about that?

Pete O'Doherty: Indeed, one of the biggest issues is where a victim reports his or her fraud and never hears back from the system as to where their case is. In many cases, in speaking to victims, they understand why the police will not investigate, but get very frustrated that no one is telling them why.

One of the main ways we are going to address that is an online portal. If you buy an item of clothing on Amazon, you can log on to your dashboard, track your order and see where it is in the system from sale to distribution and to shipping. It is going to be like that. You can log in with your crime number and you will have a victim dashboard, where we will do two things: we will interactively show you exactly where your crime is in the system, and we will make it fundamentally clear what outcome is attributed to that crime. Even if it is not an investigation, it might be some websites we have taken down. Lastly, through an improved victim care unit we will push better prevention advice to a victim based upon their individual circumstances.

Q33 **Sir Robert Neill:** Are you using victims and victims' groups to test the development of those portal systems? Is there some end user input into it?

Pete O'Doherty: We absolutely are, both operationally and as members of our programme broad, overseeing the design and implementation of this new solution.

Graeme Biggar: I just want to add to that answer. First of all, as a word from outside, I do not have responsibility for it but, in defence of Action Fraud, a lot of the opprobrium that gets heaped on it is a consequence of our collective failure to tackle the issue of fraud. That is a team that takes the reports in. It is just the first part of a broad system. There are a lot of people there working very hard to do their best to look after victims, and the flak should be at us rather than at them.

Secondly, an awful lot of the reports that come into Action Fraud have very little that it is possible to follow up on. We can do better in letting people track what we are doing with the report, but it is just a fact that very often they have no idea who has defrauded them and there is very little by way of intelligence leads that we can act on. That is why my final point is that, as Pete mentioned earlier, it is really important that we move, as we are, to being more proactive in the way we are tackling fraud. Historically, we have tried to take in reports from the hundreds of thousands of victims there are and then act on them. Actually, that does not work very effectively because of the information we get.

We are trying to do exactly the thing Matthew referred to earlier that the Met did last week. That is trying to get behind who is doing this, get behind the technology and the infrastructure they are using, and address that. We think that will do a much better job of not only providing justice for these victims—although it will be hard to say exactly who was the victim—but protecting other people from becoming victims in future.

Q34 **Sir Robert Neill:** Clearly, prevention is better. Equally, perhaps, within the new system, it is fair and honest to people to say at the beginning why it may not be possible to take the steps that they would like to be taken. It is when people are left in a sense of limbo that a degree of cynicism towards the system and towards co-operating with the police creeps in.

My final question is around legislation. Mr Tessier, you talked about the Online Safety Bill, but you will have seen that the Justice Committee report suggests that one thing that could be done, particularly because a lot of fraud is enabled through quite substantial commercial platforms here and abroad, would be the creation of a duty to prevent offence, along the lines of other offences. Partly, it would give a criminal sanction over some behaviour, but also, as we know, duty to prevent offences in other contexts, like the Bribery Act, have changed corporate behaviour. What is the position on that? What will be a suitable vehicle for that?

Duncan Tessier: I know this has been raised in the context of the economic crime Bill, which is currently going through Committee stage. I know Ministers are actively considering it. We have heard views; we have seen them in your report and others, so that is a question with Ministers right now.

Q35 **Chair:** Without straying into policy, could you see legislation working? How would it need to work?

Duncan Tessier: The Law Commission looked at this quite extensively and published its report earlier in the year, which sets out the detail of how this could work. It is a question that has been debated for the last decade.

Chair: That is the challenge. Legislation is not always the answer to everything.

Duncan Tessier: They have come up with some proposals there.

Q36 **Sir Robert Neill:** We have referred to the uplift in police numbers, but of that uplift in numbers only 380 are dedicated to fraud. It is a very small proportion. That does not suggest to me that that is going to make a lot of difference on the ground, frankly. Surely it needs more than that.

Matthew Rycroft: Part of the answer, Sir Bob, is that there is that contingent of people who will be experts in this once fully recruited and trained. There is also the possibility, through the strategic policing requirement, of Government setting direction to be followed by policing in terms of this being part and parcel of the day jobs of other police members.
That is also something that Ministers are looking at.

Q37 **Sir Robert Neill:** Making it a strategic objective would be a significant step in that direction, would it not?

Graeme Biggar: The strategic policing requirement is for the Home Office and Ministers. There are a lot of other things that play into what police forces do. One of them is what is in the police and crime plans from PCCs. In your 2017 report, you commented that a number of PCCs include it in their police and crime plans, but not all. They all include it now. We have been working with PCCs, alongside the City of London Police, to raise their understanding of the challenge and the importance of tackling it. That is positive. It will take some time to feed through into how police direct their activity.

As Director General of the NCA, I have the power to get police forces to do something, and we did a tasking in December 2019 to raise the profile of fraud and get them to focus on it. The other thing that plays on what police forces do is HMICFRS, their inspectorate, and it has done two reports over the last four years into fraud. There are a number of things now that are pressing on police forces and raising the profile of this issue, which is really important, to get them to do more, not just with the police uplift programme—the 380 you refer to—but with everyone they have working for them.

Q38 **Sir Robert Neill:** You are saying in some cases you do not need warranted officers to do the investigations, but you may need civilian police staff who have particular technical skills. That multidisciplinary approach is one of the advantages of the SFO model.

Pete O'Doherty: Indeed, so many of the fraud investigators we currently have in place, and intend on recruiting, will be a blend of police officers and police staff. In fact, most of our financial investigators who are responsible for seizing and freezing criminal assets are civilian members of staff. That helps with our plans around attraction and recruitment.

To your first point around policing, just to echo Graeme and Matthew, the first step is getting more out of what we currently have. As Graeme said, every police and crime plan now has fraud specifically mentioned. Mark Shelford, the APCC lead for economic crime, has been instrumental in doing that. We hope to see a step change in that direction.

Secondly, as you absolutely will know, the investigation of fraud is significant—it is our bread and butter—but increasingly, given the international nature and the complexity of fraud, more has to be done to empower the public, to stop and block early on, and that is why the relationship between policing, Government and industry is so important going forward. It is not so much about numbers; it is about what we use the numbers for.

Q39 **Chair:** You mentioned something I was going to raise with Mr Biggar. So much of this is now international. There are a lot of things that you are having to work with other jurisdictions on through the National Crime Agency, which can take a long time.

Maybe Mr O'Doherty can give us feedback from the frontline. If you are a police officer or police commissioner, it is 41% of all crime, so it is a big issue, but you are not going to see a result on some of these things very quickly, compared with the blue flashing lights, arresting somebody and taking a burglar off the streets or whatever. Do these long tails cause problems? Mr O'Doherty, perhaps you can answer afterwards about whether there is a morale issue at local level, because it seems there is this long-distance chain of events that does not get an instant result. You cannot see the fruit of your labours.

Graeme Biggar: You are right that there is a big international element to this. It is quite hard to pin down, but we think at least 70% of the frauds we see have an international element. It is interesting—we might come back to it later and elaborate—that the big job the Met did last week, with our support and City's support, also identified an awful lot of people in the UK who are carrying this out. We have to look internationally, but we need to look domestically too.

The tail is significant of working internationally, going through and getting evidence overseas, but that is another reason why we need to be proactive. If we start off with a crime having happened and then try to investigate it, where it has an international tail, that will take a long time. If we can work proactively with other countries in advance where we know there is a crime being committed, we can try to nip it a bit more in the bud.

Q40 **Chair:** Okay, so you are trying to move to be more proactive.

Graeme Biggar: Definitely. We have had really good relationships with Ghana and, increasingly, Nigeria. We know a lot of the romance fraud emanates from west Africa, so we are working with the economic crime elements of the police there to try to get into groups. We have worked with India. The City did a really good job with them a couple of years ago. Some of the investment fraud boiler rooms are based out there. We work with our Five Eyes partners to try to get a better understanding—America is very significantly hit by fraud as well—so that we can work together on tackling that.

Q41 **Chair:** Mr O'Doherty, does it affect morale at the frontline when it is a big international issue?

Pete O'Doherty: It does. I am going to steal a narrative used in counterterrorism policing, which is that we need every frontline cop to be a counter-fraud officer, with the ability to explain where to report and what is going to happen, to give standard prevention advice, or to investigate a crime where you might have a regular customer going into a local shop using a stolen credit card. We need local policing to be involved.

There is a morale issue because, as you say, of the length of time that investigation may take, but mainly because we have not given the training and the education to those frontline cops that they ultimately need in such a fast-changing world. We are working with the college and ourselves in the City to try to improve that level of training, but we need everyone involved because it has become such a huge problem.

Graeme Biggar: I just reflect on one of the things that the Justice Committee report says—that there is a sense of hopelessness in tackling fraud. One of our responsibilities is to demonstrate that there does not need to be.

This is a massive challenge. I might come back to why it is not quite as big as some of the figures suggest, but it is still a massive challenge. We are not doing well enough in tackling it, but I do believe, and we collectively believe, that with a bit more resource, which we are beginning to get, a bit more training and a bit more focus, going more proactively upstream, we will begin to have a significant impact on this and hopefully dispel that sense of hopelessness. This is not a problem that just cannot be tackled. We can do this.

Chair: We are going to spend the rest of the hearing discovering how you think you can.

Q42 **Mr Djanogly:** You mentioned the 41% figure, which I understand is a 10% increase since the Committee last looked at this issue only five years ago. That is clearly an exponential increase. I am sure I speak for all Members of Parliament when I say that, in my post bag, I am seeing this growing all the time as an issue.

I asked my staff to get me an example, and here is one: "We are writing since me and my wife have been scammed out of money. We have a few contact numbers of the scammers, a sort code, an account number, even 12 voice messages recorded of the scammers. The bank said because it was a faster payment they cannot help, but at the end of the day it is still fraud. We lost £4,000 because they were so convincing and the messages were threatening. I called 101. They said, 'Contact Action Fraud,' which we did, and have the ombudsman's number if needed."

Now, absolutely nothing happened. Obviously, £4,000 for this family is a very large amount of money that they could not afford to lose. My first question, before we move on to getting lost in the system, would be why an elderly couple like this has to suffer 12 abusive messages where they clearly felt forced to comply. We are talking about reporting fraud, but would it not be better if we started looking at advising people how to stop fraud happening in the first place? If they are getting 12 abusive messages, there should be somewhere they can call to help them. Surely it would be a lot cheaper and more effective from your point of view to stop it before it happened. Assistant Commissioner, why can we not deal with the problem rather than the afterwards?

Pete O'Doherty: I am really sad to hear that story, and I apologise and can empathise with those victims. For me, there are four bits of key learning from that very good example as to how we solve that. To your question, indeed, policing could, with suspect information, go and investigate, maybe apprehend someone and maybe get a sentence for him or her. But to solve that problem you need the telecoms industry to disrupt those platforms being used to target victims. Action Fraud needs to be better at reassuring the victim that we are looking at the case. On quicker payments, can that be slowed down, so we identify and manage risk, and potentially prevent that from happening?

Most importantly, to your point, we here need to do a better job at empowering the public and giving them the awareness and the tools they need to self-protect. There is a lot of work going on to do that. I know we have a new public engagement team within the National Economic Crime Centre, and we are developing a national co-ordination strategy for better comms, but that was a really good example as to where we need to improve.

Q43 **Mr Djanogly:** What should that couple have done? After the sixth abusive call, what should they have done? Should they have called the police? Would they have got help?

Pete O'Doherty: They absolutely should have phoned Action Fraud as soon as possible.

Q44 **Mr Djanogly:** They should have called Action Fraud before the fraud had been committed.

Pete O'Doherty: As soon as there was a suspicion, or something did not feel right, they could report that straightaway to Action Fraud.

Q45 **Mr Djanogly:** Statistically speaking, what would have happened if they did?

Pete O'Doherty: Without knowing more details about the case it is hard. Being honest, given the level of loss, I would say it is more likely than unlikely that they would not have received an investigation, sadly.

Q46 **Mr Djanogly:** I know someone is going to ask more holistically about Action Fraud later, but could you please just say how many people are contacting Action Fraud, how many people get some reply, and how many people get it dealt with?

Pete O'Doherty: It is a very good question. Every year, we get 300,000 victims who report straight to Action Fraud, through either the contact centre or the online reporting tools. That is the first step. That is about 27,000 victims a month. On top of that, we get an extra 600,000 crimes a year that come in from industry, where we marry up those crimes and cases to understand victims and understand offenders.

Every year, that is 900,000 crimes. They get assessed and developed. Of all of those, about 27,000 crimes a year get sent from Action Fraud and the National Fraud Intelligence Bureau out to policing and law enforcement for investigation. Of those 27,000 cases that go across to policing and law enforcement to investigate, we get about a 5% criminal justice outcome, so that is someone being charged or prosecuted. Of the 900,000 crimes, the ultimate figure for criminal justice outcomes is just below 1%.

Q47 **Mr Djanogly:** That is 1% of crimes. Going back to my example, there has been no crime; there has just been someone who has been bullied 12 times, which led to a fraud. I do not see yet how what you said is going to solve that or give any satisfaction. Should that not be immediately passed back to the local police for dealing with, for instance?

Pete O'Doherty: No, because, even though it is not a crime, that will come into Action Fraud as an information report. We will use the information in that report to do some activity. It might be taking down the phone number or working with a bank. The benefit of Action Fraud is that there may be hundreds of victims who have fallen prey to the same scandal by the same offender. We can take a step back, look at all these cases and try to get a co-ordinated response from policing to do this once at the same time.

Q48 **Mr Djanogly:** Are you saying—I think this is what you said before—that the difference will be that these constituents will be told what is going on, whereas they were totally lost in the system before? Is that your intention?

Pete O'Doherty: That is correct.

Q49 **Mr Djanogly:** When will that happen by?

Pete O'Doherty: 2024. The precursor is a new online reporting tool early next year. That will not necessarily give the better contact back, but it is 2024 that we are working towards.

Graeme Biggar: It is very distressing to hear that, and we hear these a lot. It is part of a trend that has happened on fraud: from frauds that were unauthorised payments previously—they would manage to get inside the system, work out the bank details and take the money without you being involved at all—to what are now authorised frauds, where they have pressured this couple into agreeing to transfer their money somewhere. That is one of the big shifts that we have seen over recent years. It is partly because the banks, having worked with the Government and law enforcement, have got better at stopping the unauthorised frauds, but it is really distressing when it happens.

There are two things that are also relevant to answer your question, though, which are before something gets to Action Fraud, one of which you were definitely getting at. Are we getting enough messaging out to people so they can spot what is happening to them and stop it in the first place? We have had a campaign for a number of years, initially with the Government, but largely with the banks and a bit of law enforcement, called Take Five. That was trying to explain to people, "Here is what you can do to protect yourself in the first place. Here are the warning signs to look out for if someone is trying to take money from you," in exactly that kind of scenario.

Q50 **Mr Djanogly:** Did that work?
Graeme Biggar: Not well enough, no.

Chair: Our last report was quite clear on that.

Graeme Biggar: Yes, there is more we need to do on that. I can come on to how we are looking to reform comms and make that better.

Q51 **Mr Djanogly:** But you do have public information campaign proposals in tow, do you?

Graeme Biggar: Yes, in train. I will answer the second bit and then come back to that specifically, if you would like. There is persuading people and giving them the information so they can protect themselves. The other thing that would happen, though, before it gets to Pete, is the bank being involved.

As I am sure you will find in your bank accounts now as well, if you go on and try to transfer money to someone, as this couple would have done at some point, the bank pushes at you a series of questions, which it did not do a few years ago, to ask, "Has someone you do not know tried to suggest you do this? Have they tried to put urgency or some danger into the requirement? If so, stop and think; this is probably a fraud."

Mr Djanogly: We are coming back to that area later.

Graeme Biggar: It is really important. When that does not work and people still transfer the money, there is this new system, which Matthew can talk more about, to reimburse people for it.

Q52 **Mr Djanogly:** What public information campaigns are you proposing?

Graeme Biggar: We have taken on responsibility for doing the comms over the last year. We found exactly the same as you found in 2017. There are myriad campaigns. I think you mentioned 10; in our research over the last year, we found 13. That is a challenge.

There will always be a number of campaigns that need to take place, because you will always want to put particular messages out to people who are about to get their pension, or people in different situations, but what we lack is a really successful overarching campaign. Take Five has made some progress but has not really cut through in the way we would want. When we have looked at the penetration of the different campaigns that have happened—that is research we have done over the last year—Action Fraud has the best brand recognition; about 40% of the population know of it and know what it says. Cyber Aware, which is very relevant to fraud but slightly broader, is just under 30%. Most of the other campaigns are at or below 10%, so it is not getting through.

That is the analysis we have done. That is the problem we have identified. We are doing two things on the back of that. One is behavioural analysis about the fraud journey. What happens? What are the points where people can better protect themselves or spot something is being done to them and take action to avoid it? We have had various experts looking at that.

As a result of that, we have produced a behavioural toolkit, a fraud communications toolkit, which we have almost finalised. We will roll it out to everyone who is communicating on fraud at the moment, which is still a number of people, a point I will come back to, so that we have a single authoritative analysis from Government and law enforcement of how frauds happen and the messaging that needs to get out to people to help better protect them.

It will not be massively different from Take Five, because this is still fundamentally the right set of messages: make sure you have the right type of passwords in place; spot when someone is trying to pressure you into moving money; if it happens, report it, and report it quickly. But we can get into more detail about what people can do and we will provide that toolkit to everyone who is communicating, so they can use that single authoritative pitch out to everyone.

Then the next step is to look into whether we can do a much bigger single national campaign, with something that resonates better than Take Five, that can get the message into people's heads better than we have managed to previously.

Q53 **Mr Djanogly:** Although the incidence of fraud is increasing, the NAO Report indicates that the number of prosecutions has been decreasing, or the number of fraud offences resulting in a charge or summons is falling. I am interested that, when we have been doing other inquiries, investigations have often been reduced because of covid and people not being able to talk to people or approach people. In this case, because it is mainly online stuff, I would have thought that there would have been more time spent on this type of stuff rather than going to talk to people. Why has the incidence of investigation been falling?

Pete O'Doherty: It is true that, very sadly, criminal justice outcomes have been falling. From a policing point of view, competing pressures and demands, and a lack of resources, as we have discussed today, is the first reason. Lots of chief constables I speak to say, "We can do more on fraud, but tell us what you want us to stop doing or we need more resources." That is the first issue.

The second issue, as Sir Bob mentioned before, is the changing nature of fraud, the complexity of investigating those frauds and the length of time it takes. That is why it is so important under the fraud strategy that we work with industry to do stopping and blocking earlier on. You made the point about empowering the public and, as Graeme said, giving them the messaging and the advice that they need in order to protect themselves and be more proactive in identifying these fraudsters before they hurt people, so we can take them out. But that is the main reason.

To your point around covid, we saw an increase during covid for two reasons. First, people were at home, had more time on the internet and were therefore more victimised. Equally, offenders, some of whom have day jobs, had people sat there waiting to be targeted. That is why we saw a slight decrease in fraud being reported post-pandemic. It is now coming back to pre-pandemic levels. They are the main reasons.

Matthew Rycroft: To Pete's answer to a previous question, bringing it all back to the new fraud strategy that will be coming out early in the new year, one whole pillar of that will be about increasing prosecutions and disruptions. A second pillar will be about empowering the public, as you were talking about in your previous questions. The third and final pillar will be about stopping frauds reaching customers in the first place.

Graeme Biggar: In effect, there are a number of reasons that fraud has had a smaller share of a smaller pie over the last 10 years, as police numbers have reduced. That is what we are now trying to rectify. It has also been more complex. As the Justice Committee has put out, disclosure adds extra length and difficulty to cases. That has been a challenge, which is why we need to increase the number of people doing this and remove the sense of hopelessness.

As a final point, it will not be about just doing investigations, but doing better ones and picking the ones that are going to have the biggest impact. That is my more proactive point.

Pete O'Doherty: Linking to Graeme's point on disclosure, although that is not the main reason, CPS is now doing a lot of good work around developing its specialism and skills in the economic crime business area. They have a new forum where they are sharing expertise and skills, so we can get more fraud cases through the system. That was the only other point I wanted to add.

Q54 **Chair:** Well, they need specialists at all levels. Ms Olney will come later to how we work with the public, but when we looked at this in 2017, we were concerned about the Take Five programme. At the time, I remember, no member of the Committee had heard of it. It was relaunched two weeks before our hearing. The Home Office promised that it would evaluate the success of Take Five. That was going to be due in March 2018. It was relaunched in 2017. Did you evaluate it, Mr Tessier?

Duncan Tessier: There was some evaluation of it. As Graeme said, it is quite tough to measure the impact. Since then, through the new moneys that Matthew mentioned, we have been funding the National Economic Crime Centre to carry out the review of the evidence base around campaigns.

Q55 **Chair:** If I remember, one of the metrics was whether people had ever heard of it. At the time, it was not very high. Do you have any indication of whether more people had heard of it a year after it was relaunched?

Duncan Tessier: Graeme might have the statistics on what the public think about campaigns generally, although I am not sure about Take Five specifically.

Q56 **Chair:** Much as "see it, say it, stop it" is an annoying thing, it is so annoying that it has got into people's consciousness, whereas Take Five does not seem to have done the same.

Graeme Biggar: I can write and check. While Take Five did not particularly resonate, despite lots of effort, you do get that when you go on to your bank account and go into banks. You will see the questions that they are prompting. It has not quite cut through in the way that everyone would have liked—it has not had the scale of resource put into it that that would need—but some of what it was trying to achieve has happened and people will have been protected as a result, although not enough, I agree.

Q57 **Chair:** It is interesting that, despite it being called Take Five, the website says, "stop, challenge, protect", which is three. I know there are other things, but it felt very clunky when we looked at it before.

The other thing is that in March 2017, more than five and a half years ago, there were 10 campaigns running at the same time. What is the situation? I did not do a mystery shop before this session. Every bank will have its own, but is the national campaign now Take Five?

Graeme Biggar: For some time, that has been the holistic campaign that everyone has linked into, but when we did our analysis earlier in the year we found 13 campaigns rather than 10. I am not sure that is the fundamental problem. Having the right analysis beneath it and the right messages—the "see it, say it, sorted"—is where we need to get to. In any scenario that we come to in the future, we are still going to want to have individual organisations on specific issues, out to a specific segment of society about a specific fraud, doing that work. I do not think the right conclusion would be that we just need one campaign and that we need to make sure that, next time we come before you, there are not 10.

Q58 **Chair:** It is not about the numbers. It is about the effectiveness of the message.

Graeme Biggar: Exactly.

Chair: We hear that, and I know Ms Olney is keen to come on to that a little later.

Q59 **Olivia Blake:** Mr Rycroft, I have had several constituents who have been victims of card-not-present fraud involving accredited credit card vendors. I am talking about sums of between £20,000 and £40,000, so very significant fraud. People have been passed from agency to agency, regulator to regulator, and struggle to get the police to follow through because of resources. How adequate is the financial regulatory framework behind this for consumer fraud?

Matthew Rycroft: It has clearly failed your constituents. I apologise on behalf of all of us for that. As I said earlier, it is a really important part of our response to that challenge to make sure that the new fraud strategy brings together all the relevant parts of the system—not just those of us in Government and law enforcement, but regulators and, indeed, the relevant sectors of industry. The banking sector has a very strong self-interest in ensuring that this system is improved and is absolutely instrumental in doing that, with one of the charters that we have been working on recently. We have these different sector charters and the one with banking has made some progress.

Q60 **Olivia Blake:** Do the regulators give adequate resources to each investigation, or do you feel that banks are just not bothered by this because to them it is not a significant amount of money?

Matthew Rycroft: No, the banks are really bothered by this, just as we are.

Duncan Tessier: The point I was going to make was about mandatory reimbursement. The current system for authorised push payments is based on a voluntary code, so the banks return money to victims on a voluntary basis. The Treasury has announced that, in the Financial Services and Markets Bill, there will be provision to make that a mandatory requirement to return payments to fraud victims. The PSR is now consulting on exactly how that will work. That is a really important step forward, to the issue that you were raising.

Q61 **Olivia Blake:** Do you feel that when, for example, you make a payment and it goes through a system, that part of the system should take some responsibility for the fraud, because it has allowed that to happen through its platform?

Duncan Tessier: That is exactly the logic for why the Treasury has set out the changes proposed in the Bill.

Q62 **Olivia Blake:** But it is not working for people at the moment, is it? I have people wating six years for reimbursement and fighting every agency they have been going to, to get this resolved. What would a better system of recourse look like, and is that going to be delivered by the banks?

Duncan Tessier: It is about consistency. My understanding is that about 50% of victims of authorised push payment fraud get their money back. It is very inconsistent, because it is on a voluntary basis. The first step is getting clarity about what the legal requirements are. I do think that will help, but the issues you have described are absolutely right. The whole system needs to be better, and better resourced.

Chair: We do not readily get evidence from the banks in writing on this, but UK Finance seems to have summarised some of their broader concerns. There are quite interesting views from them about who should be responsible for what. I would refer people to that evidence.

Q63 **Olivia Blake:** Do you feel that, when things do not work for victims, there is a way other than the ombudsman, which sometimes does not have the resources for its own investigations, to raise this and get it on the radar? Some of these victims are part of a wider fraud, as you said, Mr O'Doherty. It just feels like there are lots of cracks in the system and maybe we are not getting the full picture all the time on some of this. Do you agree?

Pete O'Doherty: It links into your constituent who sadly lost £20,000 to £40,000 to credit card fraud or card-not-present fraud. It is troubling to hear that one because of what has happened. We have a specific unit funded by UK Finance, and it has been in place for 20 years, which is our dedicated card and payment crime unit. They are investigating thousands of card-not-present frauds and chip-and-PIN frauds. That is their remit. They work nationally.

Getting on to your question about cracks in the system, it could be that your constituent's case has been passed from UK Finance into our specialist team, who are either investigating that specific case or investigating the network of people behind that, but with no communication back to your constituent through our unit or from banking. That is a crack in the engagement and connectivity, as Sir Bob covered before, between us as a system and victims. Hopefully you are hearing lots today about what we are doing to address that, because it is a huge priority for us.

Q64 **Peter Grant:** Mr O'Doherty, you explained a wee while ago why it is that prosecution and conviction rates on fraud cases can be very, very low. I can understand the reasons for that, but, once you have gone through the process of securing a conviction, do the courts take fraud seriously enough? Do you have a view as to whether the sentences handed down for fraud are adequate compared with the sentences handed down for other crimes?

Pete O'Doherty: No, we would like to see much tougher sentences for fraud. I know there is work going on to look at the Fraud Act, which details the maximum penalties and sentences for various offences in that Act, but sentences need to be tougher.

Graeme Biggar: Fraud sentences have increased in the last few years, but they are still very low. I agree with Pete that that does not feel right. We often spend longer investigating a fraud across law enforcement than someone gets sentenced for, having been convicted, and that does not feel right for us or for victims.

One change that is happening is to do with victim statements, which previously primarily focused on what the financial loss was and did not take into account the extent to which that loss would matter to an individual or the psychological damage that would come from that happening. That is changing, which will help judges take the right decisions on sentences. All of that matters, but only if we actually get someone in front of a court and get them convicted, so we have to do much better.

I would not want to put all the emphasis on sentencing. We have to do better in investigating in the first place and at preventing it from happening. Personally, that is where I think we will be focusing a lot of our energy, because we have to get that right.

Matthew Rycroft: We have worked with Ministry of Justice colleagues to look at the data on sentencing. You can see that, even within the existing sentences, the top end is used only very rarely. Before we look at whether we need to change the maximum length, we need to use the top end more than we do currently.

Q65 **Peter Grant:** Does sentencing policy allow for the fact that there is a high chance that fraudsters will get away with it? Is there a need to increase the penalty so that it becomes more of a deterrent? It does not matter how long somebody will go to jail for if they get caught; if they know there is a 90% chance of not getting caught, the sentence is not material anyway, is it? Do we need to increase the sentences so that the small proportion of fraudsters who do go to jail go to jail for such a long time that it is going to deter others?

Graeme Biggar: There is mixed evidence on the extent to which the length of sentences is a deterrent in crime generally, but we think one of the reasons that there is so much fraud in the UK compared with other countries—there are many other reasons, which I can come back to—is that there is not much chance of being caught. That is something that we are really not happy about and we need to change. I do not think it is necessarily just the length of the sentence; it is the deterrent in the round, which is the risk of being caught, and then the sentence. We need to fix both of those.

Q66 **Peter Grant:** While others were asking questions, I had a quick google. I just typed in "fraudster jailed". In the first case that came up, a recent UK case, the fraudster had been caught but potentially could have made £30 million from his fraud. He went to jail for less than two and a half years.

A woman was convicted of a £200,000 fraud on her second offence; she had already done time for fraud. As part of the reaction and response to that conviction, she was disqualified from being a company director for 10 years. She had breached that disqualification order, set up a fraudulent identity for herself, set up a number of bogus companies, and made £200,000. The sentence that she got for that package of offences was three years. She went to jail and there is a good chance she will be out by next Christmas.

What effect does that have on the morale of your officers, when you have put so much time into bringing that woman to justice and they know that she will probably be out of jail before your officers have finished reviewing the handling of the case? What does it do to morale inside enforcement agencies?

Pete O'Doherty: Those who are new to the business area, of course, will find that frustrating, particularly coming from other parts of policing where there are tougher sentences. But to alleviate the frustration there are other tools in our tool bag. Unlike other crimes, such as crimes of passion or retribution, the reason people do fraud is for money. The Proceeds of Crime Act is a very good piece of legislation that we use very proactively to deter suspects but, equally, to strip them of all possible assets that they have made in the course of criminality. Although, yes, the sentences can be frustrating, it is alleviated by the other work we do, to great effect.

I can give you one very quick example, Mr Grant. We had a case last year. It was an account forfeiture order, the biggest of its kind, with €34 million taken from an OCG operating across borders, laundering money through the City of London as a law firm. Money went to the police, the Home Office and the CPS to do more work. So those different tools that we use help alleviate some of that frustration.

Q67 **Peter Grant:** On a related matter, Mr Biggar, again comparing what happens to alleged fraudsters with what happens to other people going through the justice system, if a teacher or a social worker is accused of slapping a child, they do not work with children until that has been fully investigated, and rightly so. If someone is accused of certain crimes of threatening behaviour, very often the bail conditions prohibit them from being anywhere near anyone involved. I know of a case where someone has been banned from contacting their MP for over three years now, while they are waiting for the case to come up.

Why is it that, when a company director is known by the regulators to have been involved in fraud, and it is just a case of putting the evidence together in order to prosecute, there is nothing to prevent that person from continuing to be a director of other companies and very probably setting up exactly the same kind of scams?

Graeme Biggar: Honestly, I do not know the answer to that question, and it is a really valid one, so can I take that away and write? It will not be for the NCA specifically, but, in our broader responsibility, I will work out which regulator that is and speak to them.

Q68 **Peter Grant:** What does it do to morale? If you are investigating somebody, very often the investigators will know what they are dealing with, but, for obvious reasons, cannot disclose it publicly. Your officers know that they are dealing with somebody who has committed a sevenfigure fraud against innocent members of the public, and they know that that person is still running an identical business under a different name and probably preparing to scam more victims. How do you keep the morale of your people up when they know that, while they are chasing somebody for one crime, they are out on the street and committing the same crime again?

Graeme Biggar: That is challenging, but morale is, in one sense, quite strong. There are lots of things that have happened since the 2017 report that are not great. We do have a better system. We are turning the supertanker around. You would feel, if you were in City of London Police, in the NCA or in the proactive economic crime teams that we are setting up around the country, the sense that the tanker is shifting and we are beginning to get on this. We are going proactive. We are getting into people who are behind these crimes, and that is exciting for people.

There are officers who will always want to investigate drugs, guns and murders, but we also have officers and staff who really are engaged and excited by this, so morale generally is not— **Chair:** It is not as bad as we might think.

Pete O'Doherty: Our staff are really excited about what is coming over the hill: the reform to Companies House, as recommended in the Treasury Committee's report on economic crime in February; the work that the FCA is doing around the regulation of cryptocurrencies and virtual assets, which is exciting; and the work that we are doing under POCA and all the investment. We have the fraud strategy. People love the intellectually challenging nature of fraud, because every fraud is different and needs problem solving, so they are in a good place.

Q69 **Sir Robert Neill:** In terms of prevention, the HMI report and evidence to the Justice Committee inquiry highlighted an issue with data sharing, particularly between law enforcement agencies, and between law enforcement agencies and the private sector—the banks and so on. We had one witness, Adrian Darbishire KC, say that there is currently "no effective mechanism" for law enforcement to share effectively with financial or commercial enterprises to prevent offending. Do you accept that, and what is being done to rectify that?

Graeme Biggar: I only partially accept that. We have much better information sharing within law enforcement, between law enforcement and the financial sector, and within the financial sector. There are some challenges there, and Duncan might like to speak to that, but something is coming in the Economic Crime and Corporate Transparency Bill that will make it absolutely clear that it is lawful for banks to share information with each other when they are at or just below a suspicion threshold. We have done lots more on sharing information. We set up a cell during covid that had about 30 members, of which about a third were public sector.

Q70 **Sir Robert Neill:** Have you improved since the 2021 HMI report, which still found deficiencies?

Graeme Biggar: We have done lots more information sharing since 2021. We have, for example, run a pilot with two banks, where they would share with us bulk financial data, which is more sensitive than metadata or postsuspicion data, around cash-rich businesses that could be used to launder money for various crimes, including fraud, and mesh that with our data to try to identify networks that we would not otherwise have seen. That has happened since 2021.

It is still imperfect. The nirvana would be if we had a system where all the data was automatically shared and woven together, which would help us identify, for Ms Blake's constituents, the money transferring and then very quickly being laundered through different bank accounts. It would enable that to be identified more quickly than we can at the moment. There are massive legal, operational and data protection challenges in moving all the data together, so there is a way to go to get to something closer than that, but it is definitely significantly better than it was in 2017 and, I think, since 2021.

Q71 **Sir Robert Neill:** What about, in the investigation of fraud, greater use of AI? For example, we all know that City law firms use AI very much more for checking very voluminous documentation and important commercial contracts, and very often find it more accurate than the human. What is being done on that in the criminal sphere in terms of disclosure and other things?

Pete O'Doherty: That is a superb question. Breaking down automation, machine learning and AI, it is fair to say that, in the very early stages of development for policing as a service, we have seen it used for firearm licensing applications. We have seen the use of chatbots in control rooms in Canada, for example. We have a chatbot now in Action Fraud. For the lower-level, less sophisticated fraud, you can use the chatbot and report your fraud, so it is an efficient route to the system.

We would like to use AI to understand how someone was a victim, so that we can proactively and dynamically give prevention advice. These are the things that we are scoping at the moment, as well as using machine learning to interrogate thousands and thousands of terabytes of data, which is now common in so many investigations.

Graeme Biggar: In 2019 we set up the national data exploitation capability within the NCA, focused not on fraud alone but on serious and organised crime generally, which takes in bulk datasets—all the data that we have in serious and organised crime from the police national computer and police national database, suspicious activity reports, Action Fraud data, data from Companies House and from the Land Registry, and some data from banks. Inevitably, with the amount of data that is involved, we have to then use automated tools, AI and machine learning to try to interrogate that data and spot networks that otherwise we would not spot. That helps us to get more proactive. We are beginning to do that. AI gets over-talked about sometimes. It is a very difficult thing.

Sir Robert Neill: It is not a silver bullet.

Graeme Biggar: It is not, but it does help. With one part of our intelligence cell, we identified 11 new networks that we just would not have spotted if we had not done this bulk data analysis.

Q72 **Sir Robert Neill:** As the technology and the nature of fraud changes, you are going to have to be future proofing both your technology and your strategy, are you not? What are the plans to do that?

Graeme Biggar: That is exactly what we are trying to do, both on that bulk data and then on your point on disclosure. The volume of material that we now seize when we are doing investigations is huge, and the Serious Fraud Office, as you might have mentioned in your report, has been doing some good work in trialling that.

Q73 **Sir Geoffrey Clifton-Brown:** Mr Biggar, I have been listening with interest to these various initiatives that you are involved with, which is fantastic, but UK Finance says in its evidence to us: "Further legislation is needed to provide private sector information-sharing powers with the nonAML regulated sectors e.g. telecommunications, online platforms and internet service providers." Do you have the legislative underpinning to make sure that these initiatives can be properly co-ordinated with all these
various bodies that have an interest in this?

Duncan Tessier: The economic crime Bill that we mentioned earlier in the session will have specific clauses to facilitate information sharing within the private sector with Government agencies. Specifically, it is about removing the concerns that the private sector raised with us about the application of civil liability, in order to allow for the information sharing. We have worked up those clauses, in consultation with the private sector and with UK Finance, very extensively over the last two years, so we hope that they will take that really important step forward.

Q74 **Sir Geoffrey Clifton-Brown:** One point that has already been discussed is the activity of the banks. The banks are now going to have this charter whereby they have to repay these sums where fraud has been proved. Is it not easier, in many cases, for the banks simply to pay and then take no further action? What is going to cause the banks to want to take further action, which might solve similar fraud, or even that one in particular?

Duncan Tessier: There are very strong commercial incentives to not want to have to pay out money to fraudsters, and that is why the banks do an enormous amount on counter-fraud already.

Q75 **Sir Geoffrey Clifton-Brown:** I hear that, but, with large numbers of small amounts being paid out, it might just be easier to pay them out than go through all the legal rigmarole that might lead to prosecution, which is going to be expensive and time consuming for them. I really am wondering what the incentives are for banks to start to delve in, with all the various agencies, to prevent a particular fraud from happening in the future.

Duncan Tessier: They do have strong incentives. Your point is whether they are strong enough at the margin for some smaller frauds, and I can see your point there, but that would also be about the broader work that we are doing across the system.

Graeme Biggar: Speaking slightly in defence of the banks, could they do more? Yes. Would a failure to prevent offence, from where I sit, be a useful addition? Yes. But they have done a lot—and a lot more than some other sectors that we could talk about—to try to prevent fraud. They have a very clear financial incentive to do that, because they are losing a lot of money.

Because of regulation, they are having to put an awful lot of people into compliance. Some banks in the UK will have several thousand people working on compliance, so that is a big cost for them. They want that to be effective. They are then compensating an awful lot of people, when those people instruct them to pass money to fraudsters. They have put lots in place, be it strong customer authentication and two-factor authentication, or confirmation of payee, which you will have when you go into your bank account. That is big engineering that they have had to invest in to try to reduce fraud. That is the sector that we have probably collectively worked the most with, and they have made some really significant progress.

Q76 **Chair:** As you highlight, there are other sectors that we will perhaps come to. It is interesting that, the last time we as a Committee were talking about making a recommendation for lagged reporting on fraud by banks, five years and a half years ago, they did not like the idea of reporting on their fraud levels, but sunlight might be a useful disinfectant for all organisations involved.

I want to touch briefly on the costs. The NAO Report highlights the Home Office's most recent estimate of £4.7 billion, but that is based on 2015-16 data and is for individuals. Do you have an update on that estimate for individuals and also for businesses? The estimate on costs for businesses goes back even further, to 2013.

Matthew Rycroft: On the first question, we will be updating that £4.7 billion cost to individuals in the fraud strategy very early in the new year.

Q77 **Chair:** Will you then regularly update that figure?

Matthew Rycroft: We will then regularly update the number.

Chair: Every year or every six months? Every year would make logical sense.

Matthew Rycroft: I could commit to doing it annually. Businesses are much harder to measure—

Chair: Because they do not want to tell you.

Matthew Rycroft: Partly because they do not want to tell anyone, but there is a lot of literature about this, which the strategy will summarise when it comes out early in the new year.

Q78 **Chair:** Although they might not want to tell us publicly—and we had pushback on that when we were recommending it, partly because we felt that it was about consumer protection—is there not a way, Mr Biggar and Mr O'Doherty, of having businesses report privately to you, or industry bodies collating data, so that they maintain a degree of privacy? We can argue about whether they should, but, ultimately, you would then have an idea of the impact on businesses, which gives you a driver to force businesses to act if they can see what the sectoral impact is. Mr O'Doherty, you are nodding away vigorously.

Pete O'Doherty: Business reporting to Action Fraud happens mostly by banking, so we get all of that in. The issue in our system is that it is really hard to bulk report. If you are a big retailer like Tesco or Sainsbury's and you want to report 200 crimes at once, the technology does not really allow it. Part of the new system being designed for 2024 will allow the provision of bulk reporting, so we get the business scale.

Q79 **Chair:** Could you just walk us through what that would mean? If you had fraud at Tesco in Cornwall and in Rosyth, how would you aggregate that? Are you the place? Tell us how that would work.

Pete O'Doherty: We would expect that Tesco HQ would report—

Chair: It would all go through HQ, so, while it would be seen as a local crime, you would have to aggregate the data somehow.

Pete O'Doherty: That is correct, and we would want Tesco HQ to have the ability to not phone up for every single crime but to bulk report it into our system, which is work in progress. Of course, the last issue, which was mentioned before, is that, if you are a victim of a credit card fraud, you report it to your bank and you get reimbursed. Under law, the bank, and not the person, is now the victim, so if the banks do not report we do not know about the crime. We are working with the banks to try to get that into our system going forward.

Chair: We are going to come on to that a bit more.

Q80 **Mr Djanogly:** You have covered most of what I want to say, but I would just make this observation. Given the data has been so out of date for so long—you mentioned 10 years, Chair—how can you focus your very limited resources if you do not know where to focus? Presumably this is really urgent.

Matthew Rycroft: As I said earlier, not all parts of the private sector want to set out publicly their losses to fraud, which is why it is difficult to estimate the total, but there is literature about it, which we will be summarising in the strategy. We do work behind the scenes with different sectors, in different ways, in order to know where to target the effort, so it is not as though we are acting totally blind here.

Duncan Tessier: Specifically on the cost to individuals, we do have a number now, and it is broadly moving in line with the growth of fraud. We are just quality assuring that and it will be, as Matthew said, published in the strategy. There is work ongoing on that.

I want to come back to the point about the scale of fraud. Through our crime survey, we have a very good view of the overall scale of fraud in the country, so it is not like we are flying blind without knowing that. Just to be clear, sometimes people say that, because it is not reported, you do not know, but the reporting is to Action Fraud, whereas the crime survey is a representative sample of the whole country.

Chair: If you look at other examples of how sectors have changed, reporting on things like the gender pay gap and the #MeToo movement has forced organisations, culturally if not legally, to report information, but we seem to have a lag on fraud. People want to hold it a bit to their chests. That is just an observation.

Q81 **Sarah Olney:** I am looking at figure 11 on page 38 of the Report, which shows the Home Office's mapping of the evidence gaps on economic crime. It dates from May 2021, so 18 months ago. There are some really concerning evidence gaps here. I am looking particularly at risk factors for victimisation—it is disturbing to see that we do not have better information about that—and the impacts of a range of factors, including cyber-enabled methodologies.

You have talked about how there was a big increase during lockdown, and about the impact of people being sat at home on the internet. Over the last 18 months, since you completed this piece of work, what progress have you made, Mr Rycroft, on filling these gaps?

Matthew Rycroft: I will turn to Duncan and Graeme first.

Duncan Tessier: The key point on this is about how we are improving the quality of our understanding of the fraud problem, which Graeme has alluded to a number of times. A really important shift that is going on here is that we are moving upstream to really get ahead of the threat and understand the nature of the organised groups that are delivering this threat, and that is building a much richer understanding of the intelligence picture.

Graeme Biggar: There is some evidence that will be rightly and properly collected by Home Office research analysts on the overall scale of fraud in terms of the number that will be published in the fraud strategy. In terms of understanding what is happening and the intelligence basis, which the NAO Report did not quite get into, we set up the national assessment centre three or four years ago, which does assessments, like JTAC does for terrorism, across the whole range of crimes.

It has done 23 assessments over the last three years on fraud, down into the specifics of investment fraud methodologies and how that works, up to a very big report that we did in June this year, which drew on information from the banking sector and from the tech sector—we wrote it, but it was done jointly—on online fraud and the methodologies that were being used. That was our kind of overarching, capping report.

We have made a really significant step forward in our understanding of fraud over the last few years, drawing on all the information that goes into Action Fraud, but also the private sector. Like all crime, it tries to be hidden. Even more with fraud, sometimes people do not even know that it has happened to them. Then it happens online, and so it is harder to get to the perpetrators. We are a long way from having a good understanding of the crime, but it is leaps ahead from where we were three or four years ago.

Q82 **Sarah Olney:** Just getting back to figure 11, having drawn up this specific map of evidence gaps 18 months ago, you have not said anything specific that you are doing to fill any of these gaps. You have talked about the work over the last three or four years and more generally, but not specifically, having identified these gaps.

Duncan Tessier: There is a research programme that is attempting to fill all of these gaps. Matthew mentioned numbers that we are going to put into the report, which are the fruits of that analysis, in particular on the impacts on business. For example, there is a survey that has been taken on individual businesses and what their exposure to fraud is, which we are just working through the final quality assurance on.

The point that Graeme is making is that perhaps the framing of this is saying that the best way of understanding fraud is through research and analysis, which is certainly an important contribution, but we get a huge amount of understanding from intelligence gathering through the services that Graeme is running in the National Crime Agency. That is the best way of really understanding the nature of the threat.

Q83 **Sarah Olney:** Can you tell me a bit more about the role of the fraud data board in that intelligence gathering?

Duncan Tessier: The fraud data board is overseeing the drawing together of this work from within the Home Office. I am trying to draw a distinction here between the research and analysis—the academic work, as it were— and the intelligence gathering, which is a law enforcement activity. The fraud data board is seeking to get clarity on the range of numbers that we have talked about today.

Speaking to the criticism that says, "Hang on—you do not have a good enough grip of the numbers," that is what the fraud data board is overseeing, getting consistency between the different sources of information, reconciling them, and drawing together a single source of truth, which is going to underpin the outcomes we want to set out in the fraud strategy.

Graeme Biggar: If I try more specifically to answer your question, given your challenge, some of it, as Duncan says, will fall more to the Home Office. Pete and his team are doing a lot more research around victims, and there is quite a lot of investment into supporting them, which will also suck out information. Offenders are what we are working on, which is a lot of what we have done assessments on. We have done sector vulnerabilities on the tech sector and the financial sector, so we have new reports on that. On prevention and disruption, the six areas go back to the behavioural studies work that I mentioned we have done over the last year.

There has been progress on a number of these. I would not say that we are yet in the place we need to be or want to be, but there is a lot of work in hand.

Q84 **Sarah Olney:** When you say that these reports are being done, who is doing them? Is it the Home Office? Is it the National Crime Agency? Is it City of London Police?

Graeme Biggar: It depends what it is. There are some that will be done by the research analysts in the Home Office. We are all joined up and there will be sharing of data. The victim-specific reporting will be done more by City of London Police, which has the best view into that, but we all pull together a lot. For sector vulnerabilities, we get everyone involved to try to do these assessments.

I mentioned the online fraud one. We had techUK and then lots of different tech companies trying to feed into us as much as possible, as well as the insurance sector and the banking sector, giving us information, which we then weave in with law enforcement data, both here and internationally. We then produce our overall assessment. The online fraud one was about 20 pages, and they vary in classification, depending on what level of intelligence we put in. Some are at official level; we will still circulate to the tech sector and the banks, so that they know, but we do not put them on the internet so that the fraudsters know what we are doing.

Q85 **Sarah Olney:** How effective is the sharing of intelligence, among not just the agencies represented here today but the private sector and the technology companies? How effective is that in terms of making sure that you have all the information that you need?

Graeme Biggar: It is pretty good with banking, I would say. There is still an issue about how many crimes they report that Duncan alluded to, partly because they have been working on this for years and have lots of people working on it. With the tech sector, it has been a lot harder. That is not necessarily through lack of willingness; this is just a topic that they have not been engaged with for over a decade, as the financial sector has. They have not collected the information, so it is very hard for them to summarise and provide it to us in a useful way. That is an area that we need to really keep working on.

I am sure that you will come on to it in your further questioning, but they are just fundamental to the way that fraud happens these days. They are massive organisations and have a huge responsibility that they need to live up to. We are working with them through a number of mechanisms, which I can come back to. We have some information from them, but there is more that we need.

Q86 **Sarah Olney:** I wonder if you could elaborate on that a little. What is it that the tech companies are not doing and what is it that needs to change? Is it new legislation? Is it a different culture within the tech sector? Is it more robust mechanisms within the Home Office or the National Crime Agency? What is it that is needed?

Graeme Biggar: It is all three of those things and the legislation. Matthew and Duncan might talk about it, but we have the Online Safety Bill coming, which has been really important. We worked hard with lots of operational partners to set out why we felt it was really important that fraud, both paid-for advertising and user-generated, was included in the Online Safety Bill. That was a long discussion and debate with Government, but we are in the right place now.

It is absolutely about us being better at engaging with the tech companies, but there is definitely more that they need to do too. It is a range of different parts of the tech sector. I can get into that now or later, depending on how you want to run the session.

Sarah Olney: Now is good.

Graeme Biggar: We have all the companies that are hosting websites, which are not your Google or your Meta, but other providers. We are working with them and with the National Cyber Security Centre to make sure that, when we can identify a website that is, effectively, fraudulent—and we see a lot of investment fraud scams happening that way—it is taken down. We do not have the power to just make that happen. We cannot offensively just take down a website, but what we can do is go to the people who are hosting those websites and say, "This will break your terms and conditions. Please take it down."

Q87 **Sarah Olney:** So you are relying on the civil law there rather than criminal law. Is that right?

Graeme Biggar: It is not even civil law; it is the company's own terms and conditions about what it wants to have up.

Sarah Olney: It is contract law, essentially.

Graeme Biggar: Yes. By and large, those are in the right place. The Chair mentioned crypto scams and currencies earlier on. Over the last couple of years, with NCSC, we have identified and taken down just over a million websites that were purporting to be crypto investment and were, basically, crypto investment scams. There is that part of the tech sector that hosts websites.

There are then all the social media companies: Meta, Google and the like. One really important thing that we have done—and the Financial Conduct Authority needs to take a lot of praise here, because it has absolutely driven this through and it has been hard yards—is to ensure that tech companies such as Google and other people who do search check, before they put in their paid-for advertising, whether the company that is trying to advertise an investment product is regulated by the FCA. That did not happen previously, so fraudulent investments were coming right at the top of Google and other providers' search results, with no checks from the company involved.

That was probably 18 months of very hard negotiation and pressure from the Financial Conduct Authority to persuade first Google and then the other companies to put that mechanism in place, and that has been a really important step forward. You are much less likely to see a fraudulent website, certainly in paid-for advertising, than you were two years ago.

Then you have the social media companies like Meta and Instagram, where lots of user-generated frauds were being pushed or romance frauds were started. We see a lot of that too, and that is probably the harder area. They will tell us that they take off a lot of fraudulent websites and personas all the time, but it still feels like a lot is getting through. Some of that is the same challenge that the financial sector has had, as we have, for the last decade, in that, as soon as you put a control in place, they will try something else. You put two-factor authentication in place, and then they move to authorised push payments, so that they are getting the victim to do it themselves. Of course, that is what we see in the tech sector.

They do put changes in place, and then a way around it will be found, so there is an element there where we just need to keep on understanding the methodology, finding a solution to it with the tech sector and getting them to implement it, accepting that something else will happen and that we need to be on to it as quickly as possible. There is a level of co-operation with the tech sector that we are at the start of a journey on. It has been the last two years, whereas we have been doing it with the banking sector for a good decade or more.

The mechanism through which we do it is the online fraud steering group, which is, effectively, jointly chaired by the NCA, UK Finance, which the Chair mentioned earlier, and techUK, representing the tech companies. Around the table, we have various law enforcement partners—City, the National Cyber Security Centre and so on—the tech companies themselves, or their UK representatives, and the major banks. That is where we are trying to bring together these issues and drive it forward.

Q88 **Sir Robert Neill:** What is the fall-back position if, at the end of the day, all these voluntary agreements and charters do not work?

Graeme Biggar: The Online Safety Bill will not be voluntary and will have significant penalties attached to it. As Duncan mentioned earlier on, for the banks, the contingent reimbursement model—paying someone back if they have been victim of a scam where they authorised it—is going to go compulsory. At the moment, about 50% are repaid, but that will move up to 100%. Those two things are moving from voluntary to compulsory.

As I said earlier, from the NCA's point of view and that of a lot of my operational colleagues, we would also welcome a failure to prevent offence, for exactly the reason that you mentioned earlier. It is not that we will end up doing lots of prosecutions of major corporations—

Q89 **Sir Robert Neill:** It changes behaviour, doesn't it?

Graeme Biggar: It will, as it has done with bribery and with tax evasion, change the behaviour of the companies, to make it less likely that it happens in the first place, which is of course what we want.

Q90 **Sir Robert Neill:** The other thing that struck us was that the NECC raised concerns about the comparatively slow pace of developing international relationships. Of course, 80% is online, and a huge chunk of that is enabled abroad now. We seem to have been quite slow out of the traps in building international relationships, for various reasons. Given that that international element is not going to change any time soon, what is the plan to increase the extent and the intensity of the international connections to tackle this?

Graeme Biggar: That is a really fair challenge. On a number of points that you have raised, I have said that it is not quite as bad as you think, even though we have more to do. This is one where we really do have a lot more to do. There is not quite the international mechanism on this. On money laundering and terrorist finance, Duncan will remember how many years ago, but the Financial Action Task Force was set up at the behest of the G7—or G8, as it might have been at the time—and has provided the mechanism and forum to try to drive up performance on money laundering. We have not had an equivalent on fraud to dock into, so there is not really a multinational mechanism for operational law enforcement partners like us or policy colleagues to drive improvements across the world.

We collectively need to reflect on that, but we can, in our own sectors around law enforcement, do more internationally. We work with the Five Eyes and, as I said earlier, with the Ghanaians, the Nigerians, the Indians— and the Emiratis. That is a really important country for us, as a lot of money laundering goes through there, as it does through London. So we know where we need to work with, but we need to do more on that and to find a better multinational mechanism to do it.

Q91 **Sir Robert Neill:** As far as you are aware, have Ministers raised this in discussions with their international interlocutors as a priority?

Chair: Mr O'Doherty seems to know.

Pete O'Doherty: I just wanted to respond to the initial question. Forgive me.

Matthew Rycroft: We can write with the specifics, but what I hope that you are hearing from all of us in our different ways is a sense that the whole of the system needs to be operating in a step-changed way to step up to the scale of the challenge. The fraudsters are very good at spotting the vulnerabilities within the system. Parts of that system have progressed more quickly than others.

Chair: We are talking about the international point, though.

Matthew Rycroft: The international part of the system is as crucial as the rest, and that is why, as Graeme said earlier, we are working in collaboration with our partners, who are not just the traditional Five Eyes partners. You mentioned Ghana, Nigeria and many others, but that whole side of things needs to step up as well. We will write to you on the Ministers.

Q92 **Chair:** Specifically, we are a member of the Commonwealth but we are not a member of the EU any more. Does not being a member of the EU make a difference? We know that there are difficulties in sharing information between the Home Office and other jurisdictions.

Matthew Rycroft: We have got around that set of issues with our postEU exit arrangements.

Q93 **Chair:** So you are confident that you have got around everything that you need to get around in order to share data on fraud in particular.

Matthew Rycroft: We have got around the issues about leaving the EU, yes.

Q94 **Chair:** There are still Departments that struggle. For instance, DEFRA is struggling to get information about dangerous things in the supply chain. It has to scan the media to get some of that information, because it does not have the same protocols.

Matthew Rycroft: On law enforcement, we have the right mechanisms in place and are now using them.

Q95 **Chair:** So we are not at any detriment. You say that we have got around all those hurdles.

Matthew Rycroft: There is much more to do with our international partners through the mechanisms that were set up and are working in order to get better outcomes on fraud. None of us on this side of the table is at all complacent that everything is comfortable. We know that we need to go further and to step change, including with our international partners, but also with the sectors back home.

Q96 **Chair:** Just to be really clear, Brexit has not led to any gaps in our knowledge about what is going on or any interaction issues with other European nations.

Matthew Rycroft: Before the UK left the EU, we had set up the mechanisms to deal with that challenge.

Q97 **Chair:** There are mechanisms, but is there any detriment? We know that there are mechanisms and workarounds, which can be a bit clunky and a bit slow, and we have a time lag. I am thinking about some other Departments in particular. In terms of fraud, you are getting it all in real time.

Graeme Biggar: I can give an operational take on it, if it is helpful. I cannot think of anything that has stood in our way on fraud, and we are working really well with Europol and Interpol.

Chair: That is what I just needed to be really clear on.

Q98 **Sir Robert Neill:** Will there be specific elements of the new national strategy that deal with the international element? Will there be specific tasks, objectives and timelines to improve the international element?

Duncan Tessier: Yes.

Sir Robert Neill: Perhaps you can set those out when you write to the Chair.

Matthew Rycroft: The whole thing is not quite ready to launch yet, which is why we are giving this evidence without being able to tell you everything that is in it. I can assure you that there will be plenty on this side of things.

Pete O'Doherty: If we are going to work upstream and have an impact on fraud, building the mechanisms, as Graeme said, and the infrastructure to work internationally is important.

Equally, just to reassure you, some really good bits of work are going on internationally. We have been out in India with Microsoft, challenging the contact centre issue from India around computer software service fraud. We have been doing lots of work with west African countries around romance fraud. In fact, loads of active operations are ongoing as we speak.

We have a relationship with advertisers globally, removing advertisements from some websites. Counterfeit goods, for example, is a wider economic crime issue, not just a fraud issue.

We are removing payment enablers from websites—Mastercard, Visa, Worldpay and PayPal—so that moneys cannot be laundered overseas. We have offices in the US managing transatlantic money laundering. It is about industrialising and doing this at scale, but certainly the NCA, as the system lead, and the National Economic Crime Centre, in the work that they are doing, are confident that they will see lots of good progress in the next few years.

Q99 **Sir Robert Neill:** Do we do anything to help those countries strengthen their own capacity, because some of that can be very variable?

Pete O'Doherty: Interestingly, through our Economic and Cyber Crime Academy, we sometimes do capability building in overseas countries, particularly around our money laundering and fraud investigations. To be honest, I am in the process of scaling that back, because I need the academy's capacity to be training this uplift of officers and staff coming in under the fraud reform programme in the next few years.

Graeme Biggar: One example on that is in Ghana, where we have been working on capacity building in co-operation with the very effective force that they have there. One thing we have rolled out with them is training in schools about fraud awareness, because it has been, in that society, a fairly attractive career to go into. We are trying to tackle it right at the root of it, absolutely with their co-operation.

Q100 **Sarah Olney:** I want to talk a little more about Action Fraud, Mr O'Doherty. There has been lots of criticism, including in this room, about Action Fraud and its services so far. Can you tell us what the City of London Police has been doing to respond to some of these criticisms? What do you identify as the failings and how are you addressing them?

Pete O'Doherty: I will start by echoing Graeme's point. The reason why there has been no action in Action Fraud is, first of all, the technology and the service that we give members of the public. Secondly, no matter how good Action Fraud is and how easy it is to report, even if we contact our victims more, we need the infrastructure behind it that does all the investigation, the prevention, the comms and the disruption work to be more effective. That is the starting point.

To answer your specific question, it is primarily about procuring a new technology for 2024. We have built an economic crime victim care unit, so we recognise that, given that there are so many victims who do not receive an investigation, we need to do more work around giving them support and prevention advice. The economic crime victim care unit contacts both nonvulnerable and vulnerable victims to give that prevention and support. We contact about 7,500 victims every four weeks. That is being rolled out to every police force in England and Wales over the next two years.

Another piece of work that we have been doing is around how, if we cannot do more investigations, we prevent repeat victimisation. We know 17% of victims fall victim at least twice. We have a whole team that is extracting what we call cyber-enablers—telephone lines, email addresses and websites. Graeme talked a lot about this before. Through relationships with industry and Government, we provide intelligence every day, and get those entities disrupted and taken down, so that they do not harm any more people.

Lastly, it is about trying to get more cases out to policing more quickly, so that those lines of inquiry are fresher and incentivise the police to take on more investigations.

The very last point that I would make is around using some of the data in our system to do weeks of action on things like investment frauds, courier scams, which we know are a big issue, and romance frauds. We work under the leadership of the National Crime Agency and the NECC, across policing, for a week of action, where we target, disrupt and enforce some of the most serious people involved in these crimes. One recently was Operation Henhouse. Under the leadership of the NCA, 186 people were arrested and we recovered over £33 million of criminal assets. These were people impacting victims here in the UK.

Q101 **Sarah Olney:** With Action Fraud, one weakness that has been identified is that it is not as effective as it could be in capturing data about fraud, partly because victims do not know about it, and secondly because the system itself is not user friendly. When you are recommissioning or going out for the new system that is coming online in 2024, how will you address those weaknesses?

Pete O'Doherty: It is the level of information that we get from victims at the point of reporting, and using intelligence to understand how the crime has happened as opposed to just what the victim says. As an example, for romance fraud, we have seen a real trend where the suspect claims to be a soldier serving in the American military and is phoning the victim from the US. When the victim reports it, the suspect is John Smith. He is a soldier and works in the US, but, of course, he is nowhere to be seen. We need to use our relationships, share data and develop that investigation to say that romance fraudsters are operating from X and are not in the US. It is about getting better information from victims. It is about bringing intelligence in from the private sector, the tech companies and law enforcement, so that we have a better understanding of how offenders are committing these crimes.

Q102 **Sarah Olney:** Are you confident that some of the poor experience that victims have had with Action Fraud—the Report mentions things like Action Fraud staff mocking victims—is being addressed?

Pete O'Doherty: Definitely. We were very embarrassed and frustrated when that happened, and lots of work has been done to improve that and absolutely prevent that from happening ever again. That has been built into the way in which we have approached the procurement of the new services. All the learning from before has fed into our leadership of this new procurement process.

Q103 **Sarah Olney:** The Victims' Commissioner, in giving evidence to the Justice Committee, talked about how Action Fraud is not a victim-centred service. Can we expect to see that improve? What will you be doing during the procurement process to ensure that it is a much more victim-centred service?

Pete O'Doherty: There is a range of things that we are doing to improve that for victims: first of all, using victims to help test the design of the new solution; reducing call waiting times, so that we drive down abandonment; having that user dashboard, so that you can log on and see where your crime is in the system; doing our very best to attribute an outcome, even if it is not an investigation, so that they feel reassured that there was value in them reporting this fraud; continuing to roll out the economic crime victim care unit, so that as many victims as possible get that afterreporting care from us around further prevention.

Q104 **Peter Grant:** We have one Government Department and two public agencies here. We could easily have filled the witness table three times with Departments and public agencies that have a major part to play in the fight against fraud. When was the last time that all of those Departments and agencies sat together around the same table or on the same Zoom call and spent time talking about fraud?

Duncan Tessier: We held the joint fraud taskforce a couple of weeks ago, which the Security Minister chaired. We had a Treasury Minister there and DCMS representatives, as well as the private sector—the financial sector and the tech and telco sectors. We discussed bringing together the fraud strategy, measurement of success, what outcomes we were trying to achieve, and progress, particularly on the sector charters that Matthew mentioned earlier. We regularly bring those groups together. I absolutely understand the point. It is a large number of stakeholders and it is challenging to get governance to make that work, but we do a reasonable job of it.

Q105 **Peter Grant:** Would you be able to write to us with details of who attends? ***Duncan Tessier:*** Yes, absolutely.

Graeme Biggar: That is one meeting, and a really important one. I can see where you are going to go with this. We do have lots of meetings, but we need to. Beneath the joint fraud taskforce, we have the fraud strategic governance group, which is chaired from within the NCA. We will have a bigger series of operational partners around the table than can fit at a joint fraud taskforce meeting. We had the last one of those a month ago. That is one of the big things that we have been doing over the last two or three years.

Indeed, one of the things that you and other Select Committees have argued for is making sure that we get the right people in the room, and it is an awful lot of people—it just is, because fraud touches on so many different parts of society. That does take governance and that does take a lot of meetings, which can feel confusing, but it is absolutely necessary if we are going to get the broadest reach around the problem and make the difference. Anything that we can do—and Duncan and team have done a bit—to simplify the governance is welcome, but it will always be big and complex, with really big tables with lots of people around them.

Q106 **Mr Djanogly:** On the interaction with the private sector, Sir Bob was asking what happens if voluntary charters do not work. Can I just, maybe for my own benefit, understand how you are going to be reviewing these on an ongoing basis? When will that happen and when will there be feedback to Parliament, so that we can keep an eye on what is going on with these voluntary charters?

Duncan Tessier: As I just mentioned, one of the key aims of the joint fraud taskforce is to oversee the implementation of the charters. The meeting that we had just a couple of weeks ago went through the progress against the three charters that have been issued so far.

I would point out that one of those was the telecoms charter, where one commitment that the telecoms companies made was to introduce new software to try to reduce the number of spam text messages. We agreed that with them 18 months or so ago, and they have made some really dramatic progress through that work. They have seen scam text messages on some of the operators fall by over 90%. That is just a practical example of how this voluntary approach can work. I absolutely appreciate the points made, though.

Q107 **Mr Djanogly:** How does Parliament find out what is going on in the joint taskforce?

Duncan Tessier: We are very happy to write you and set out the progress against that. There will be a commitment in the strategy to deliver against that as well.

Q108 **Chair:** Can I suggest that we work with you and with our colleagues at the National Audit Office to find a way that you can report all of these different groups? There is international, there is—Mr Biggar gave us an alphabet soup of some of them. It would be helpful to have it in one place, in an easy-to-read dashboard, for Parliament and the public to see what is happening. One of the challenges that we have had since we looked at it in 2017 is how you follow through on these many strands.

Matthew Rycroft: The strategy that, as we have mentioned several times, is coming out early in the new year will answer some of that question and will set out milestones.

Q109 **Chair:** We have worked with other Departments to frame how that report to Parliament is made. With the best will in the world, Mr Rycroft, what Whitehall thinks Parliament wants is sometimes different from what Parliament wants, and it will make your life a lot easier if you give us what

we want in the first place.

Matthew Rycroft: We are all ears about what Parliament wants.

Chair: Fantastic. We love it when Whitehall is listening to Parliament.

Q110 **Mr Djanogly:** In the same vein, I am looking at the written evidence submitted by UK Finance, which is somewhat top-heavy on what Government can do for them, rather than the other way round. That being said, in paragraph 9, they say: "In our opinion, the Joint Fraud Taskforce does not currently have a sufficiently broad mandate to provide strategic oversight of fraud risk management activities across all sectors. To date its focus has been limited to the three Fraud Charters and existing workplans. It does not have a credible or effective delivery mechanism to ensure oversight of a co-ordinated fraud response across sectors. We would encourage the Government to re-evaluate the continued focus on the Charters given the advent of the Government's Fraud Strategy. Instead these should be superseded by a public-private cross sector strategy with effective oversight provided by a strategic board, ultimately reporting to the Economic Crime Strategic Board." Have you seen this submission?

Duncan Tessier: I have not seen the submission. As Matthew has just said, we are bringing together a system here, and you can hear all the different parts that have been identified. They will be set out coherently within the fraud strategy, which will have the clear milestones, and then we will monitor and deliver that through the joint fraud taskforce, which would speak to the concerns being raised there.

Q111 **Mr Djanogly:** You would agree with my view that they are not exactly totally enamoured with the joint fraud taskforce, and that does not totally point well towards joint working with the private sector.

Duncan Tessier: We have had really good engagement with them on the joint fraud taskforce.

Mr Djanogly: You do not know where this has come from.

Duncan Tessier: They are really keen to see a holistic strategy set out, which they can see measurable deliverables against and can track progress, which is exactly the thing that the Chair has just asked for as well, so we are all on the same page on that.

Q112 **Sarah Olney:** I have a quick follow-up on what we have been talking about in terms of the public and their experience of fraud and how it is investigated. Like everyone here, I get a lot of constituent correspondence on this—some really distressing stories. What Mr Djanogly and Ms Blake have already highlighted are just examples, really, of what we all hear.

It strikes me that, certainly for a lot of my constituents, being a victim of fraud is their experience of being a victim of crime and often tends to be their only touchpoint with the police in terms of reporting. When they get a bad experience, that really colours their perception of the police overall and the approach to fighting crime, and they can have a very negative opinion—often, certainly as far as my local forces are concerned, a really undeserved negative opinion—of the police and how effective police forces are at fighting crime.

This is probably a question for Mr Rycroft, since, Mr O'Doherty, you represent only a single police force, even though you are here to talk about fraud. I just wonder to what extent it is important to you to get this right. It is such a massive issue for the public, particularly in the way it colours public perception of the police.

Matthew Rycroft: It is a huge issue for me and for us. You have absolutely put your finger on why it is right that we are investing so much more in Action Fraud as the main interface between individual members of the public who are or think that they might be victims of fraud, and the policing system. We know that Action Fraud's performance was not good enough, which is why Peter set out all the myriad improvements that are in train.

There has been some progress since then, with much more to come throughout next year and up until 2024, when the new system will be fully up and running. In the meantime, we are seeking to ensure that that touchpoint, as you put it, is as good, sympathetic, victim-centric, victimfocused and victim-friendly as possible, given how distressing it is for so many of your constituents and many others when they go through this sort of fraud.

Q113 **Sir Geoffrey Clifton-Brown:** Assistant Commissioner, I would appreciate a really candid answer to this question. You are the lead police force. How good is the co-operation between you and the 42 forces, and is it variable?

Pete O'Doherty: The co-operation is strong, but the issue is the resourcing. The friction sometimes is that, because we are the interface, as Matthew described, we are sending out thousands of crimes to policing, but nowhere near enough is getting investigated. We are frustrated by that. They are frustrated, because they want to do more, but they do not have the people or the resources.

In terms of relationships and co-operation, it is very strong. I will give you one quick example. Where we identify a big fraud problem, which might be a certain type of investment scam or romance fraud—something that is really affecting the UK public—the police service is very good at downing tools, stepping up and supporting us on that week of action or national campaign with Government and the NCA.

The co-operation is really good. It really is a resourcing problem. Chief constables in particular want to do more on fraud, but they do feel a bit under pressure in trying to solve issues around violence against women and girls, human trafficking, county lines, serious and organised crime, and terrorism. They just feel under pressure, but they all very much welcome the work that we are doing, whether it is legislation on online harms, the resourcing that we are doing or the fraud strategy, and are excited about what that will mean in terms of servicing their local people much better than they currently do.

Q114 **Sir Geoffrey Clifton-Brown:** I hear that answer. How much would the individual police constable on the ground know about fraud? Would he know that you are the lead authority, and would he benefit from some better training?

Pete O'Doherty: The constable on the ground will know very little about fraud. They probably will not know about the national lead force status and, if they do, they will know very little about it. They definitely need more training. How are we managing that? We are in the process of launching a fraud app that is available for constables on the ground. If you are on the street and you are engaging with the community or a business, you can log on. It describes what Action Fraud is, how to report fraud, what the national lead force does, what it means and what the NECC is, and it gives sample prevention advice narratives that they can give to members of the public.

Q115 **Sir Geoffrey Clifton-Brown:** Mr Rycroft, it does seem that police forces need to have fraud as a strategic objective, so that these issues can start to be addressed and that individual chief police officers have to balance what they do on fraud. Given the severity and value of it, it needs, surely, a much greater concentration by the individual police forces, which involves the Home Office giving that strategic lead and giving them the resources that they need to do it.

Matthew Rycroft: Absolutely, we have heard that message loud and clear, not just today from this Committee but from many others in the sector. I am hopeful that, with the next iteration of the strategic policing requirement, which sets out, from the Home Secretary, the overarching top priorities for policing, this issue will have been progressed. We just have not quite got there yet, which is why I am talking the way that I am.

Pete O'Doherty: Although, of course, we need policing to do more investigations, we all need to work differently. We have spoken about being more proactive and being intelligence-led, so getting them the right intelligence and the right packages quickly, and trying to take out these fraudsters before they hurt people. Everything that we are collectively building is to that ambition.

Q116 **Sir Geoffrey Clifton-Brown:** Mr Rycroft, I started this hearing not knowing a lot about this subject. I have come through the hearing realising how complex it is and how many bodies are involved. Does the Home Office, with all its other difficulties at the moment, have the bandwidth to really get on top of this subject, given the seriousness of it?

Matthew Rycroft: Yes, we do, because we have clear governance and clear accountability. As I said, the Home Secretary is ultimately setting the direction for the whole Department. Of course, the Security Minister is the Minister for tackling this and has it very high up his list of priorities. At official level, Duncan is the director, and his director general is also very focused on this, as am I. It is a very complex bit of system leadership that is required, but that is what the Home Office does. We do that in other types of system as well, and we are learning lessons from those other systems and applying them to this one, given that it is relatively less mature than some of the other systems.

Q117 **Sir Geoffrey Clifton-Brown:** I do not want any criticism implied in this question, but, given the seriousness of the types of crimes, do we have the correct institutional bodies involved? I do not want any criticism of Mr Biggar involved in this, because he has been an excellent witness and his organisation is doing a very good job, but do we need to simplify the governance, which seems from figure 9 on page 32 of the Report to be very complicated? Mr Biggar has an awful lot of other things to do, so should we be considering having one specialist national fraud agency looking at this very serious category of crime?

Matthew Rycroft: The way that I would think of it is that we have a national fraud agency but we do not call it that. We call it the National Crime Agency, which is our national agency for doing fraud—

Sir Geoffrey Clifton-Brown: But it has lots of other jobs to do.

Matthew Rycroft: —alongside other aspects of serious and organised crime. There are benefits in the different crime types, when they are serious and when they are organised, being treated through a single agency. Of course, we need to strengthen the National Crime Agency still further, and Graeme and I talk very regularly about how we are going to do that through resourcing, and through its relationship with the rest of law enforcement and the intelligence community, for instance, but we are determined to make further progress in that direction.

Q118 **Sir Geoffrey Clifton-Brown:** If we were sitting here in a year's time doing another inquiry, how much improvement would we see in this area?

Matthew Rycroft: First of all, we will be tracking very specifically the outcomes set out at the beginning of next year through the strategy. You will be able to hold us to account to the milestones that we will have set out earlier in the year and how far we have come through that first year. I would not have expected, in that time, the proportion of total crime that is fraud—the 41%—to have reduced, but we are aiming to reduce that figure in time. That is going to take a long time. One of my colleagues was talking about the super-tanker, and it really is. It is very hard to make instant inroads into these very thorny problems, but we will be throwing even more attention and resource at this question in a year's time.

Q119 **Sir Geoffrey Clifton-Brown:** As a final question, I am really concerned about the Assistant Commissioner's answer to me that the individual police constable on the street will know little about fraud crime. That surely has to be urgently addressed.

Matthew Rycroft: I totally agree. That is the bit that needs to be addressed through an elevation of fraud up the national list of priorities for policing.

Q120 **Chair:** But also for other organisations that interact with people, such as consumer organisations. Mr Biggar, we were talking earlier about how much fraud there is and you said you would come back to that. We talked about the numbers, and Sir Geoffrey has also highlighted how quickly there will be progress when the new strategies come out. I am sure that you will agree with the Permanent Secretary, because you are sat next to him and that is what usually happens at these events, but when do you think we will see a reduction in the amount of fraud that is perpetrated?

Graeme Biggar: We just have, and this is why I am feeling slightly unsettled in answering this question. If you look at the crime survey for England and Wales, rather than the reports to Action Fraud—although, as it happens, they have also gone down—we had seen a steady trajectory and were thinking about how we could try to take action that would reduce the scale of growth of fraud, given the challenges we were facing. The figures came out from the June 2022 crime survey for England and Wales, and we saw a drop from 4.5 million to 3.8 million. That is quite a substantial drop in the number of frauds that were being reported by members of the public in the crime survey for England and Wales.

We had not quite seen that coming. We are pretty confident that it is accurate and that the methodology that the ONS has used is correct. We can retrospectively hypothesise about why it happened, and a good part of it might have been what Duncan spoke about earlier—the really good work that the telcos have done to reduce the number of scam texts going out.

The other point I want to make is about trying not to have a sense of hopelessness around this. While 3.8 million frauds sounds like just an extraordinary and impossible number, in 36% of those there was no loss from the fraud: a scam text was sent but nothing was done with it; someone did phone up one of your constituents, but they did not act on it, so nothing happened. It is still really important that we know it is happening, and it is still a concern, but no fraud took place. Then you have the other 64% that will have had a loss, but two thirds of those, or 40% of the total, were reimbursed, so you are down to 24%.

Q121 **Chair:** If it is reimbursed, there is still a victim.

Graeme Biggar: Yes, absolutely, and there is still a criminal getting the money, so I am not saying it is not important. I definitely think we need to be doing more on this.

Chair: But in terms of protecting the individual victim—

Graeme Biggar: Just in terms of understanding where it gets really significant. Where there is a loss, the median loss from frauds that got reported to the crime survey for England and Wales was £79, which is still really significant to some people—I am not pretending that it is not—but you get into life-changing amounts of money when it gets into the investment frauds and the romance frauds.

Q122 **Chair:** But each £79 adds up for the person who is collecting the £79.

Graeme Biggar: It does. I am not trying to diminish the challenge. It is very significant, but, as we try to get into it, we need to avoid that sense of hopelessness by picking it apart and seeing where the damage is really coming and what is the most significant.

Q123 **Chair:** I am sure that you do not mean it this way, so maybe you would just like to be clear on the record, but it does sound like, if you are a scammer and you go fishing for £1 here, £5 there or £79 there, you guys are not going to go for them, because it is not big enough. What is your message to people on that?

Graeme Biggar: Absolutely not, and that is part of us going proactive. What we will not be able to do, probably in capability but certainly in capacity terms, is launch a major criminal investigation reactively if someone has been defrauded of £5. We can, as I mentioned earlier, try to be more proactive. I will give you 60 seconds on what the Met did last week, because this is a really significant part of what we are collectively trying to do.

They had identified, with us and other partners, including one in the voluntary sector, a website that was helping criminals to make spoof phone calls to individuals. They would be called and they would think it was coming from their bank, the NCA or a Government Department, but it was coming from a criminal. That is a fantastically important tool to have if you want to defraud people.

They had identified the website that was doing that, and then, with our help, penetrated it and identified who were the victims of it, or at least the phone numbers; we have got a bit of a challenge then getting to the individuals. From that, we have identified 560 suspects within the UK, so this is not all international. We sometimes, as I said earlier, think it is all international, but it is not. Over 100 of them have been arrested already. These are the users of the website, along with the person who ran the website.

If you go on to the website now, you find a wonderful video that Met comms colleagues need to be applauded for, which says, "Welcome to iSpoof"— the name of the website. "Log on here. Give us your criminal intent. We are law enforcement. We are taking all your details and you will soon be getting a knock on the door."

It is a very humorous read, but it is not just humorous for the public. It is a brilliant deterrent message for criminals that they need to be worried that, when they are going on to different bits of websites, be it in the open web or the dark web, we might be there and might be operating. That is how we will get to some of the people who are doing the £1 or £5 frauds as well.

Q124 **Sir Geoffrey Clifton-Brown:** Mr Biggar, you just struck a thought in my mind. Why can you not produce that sort of training video for every single police officer in this country?

Graeme Biggar: In terms of sharing it with police officers in the country, it is quite an empowering video to see.

Chair: It sounds like we are all going to go and have a look at it. You need a teenager to put it on TikTok.

Graeme Biggar: Someone forwarded it to me on Twitter, because it had gone a bit viral.

Chair: There are so many more questions that we would love to ask, but our concern here was that we looked at this five years ago and it still feels like this super-tanker you were talking about, turning and chasing speedboats, and it is a very difficult task. We recognise that, but we are, as you perhaps reflect, frustrated about slow progress here. While we want power to your elbow to deal with this, we will be watching this very closely, and it cannot all ride on the legislation.

There are so many other questions that we would ask if we had the time, but we are also considering what to do with our sister Committees. Justice has looked at this, and we have looked at it before. Other Committee Chairs and I have been in discussion at early stage, so watch this space. We may have you all back in again for a super-hearing at some point.

Can I thank you for your time? The transcript will be put up on the website, uncorrected, in the next couple of days. Thank you to our colleagues at Hansard, thank you to the National Audit Office for its excellent work, and thank you to our witnesses for their time today. Our report will be published in the new year.