Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 16 June 2022

9.30 am

Watch the meeting

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

Evidence Session No. 20 Heard in Public Questions 212 - 221

Witnesses

I: Assistant Commissioner Pete O'Doherty, City of London Police; Rob Jones, Director-General, NECC/Threat Leadership, National Crime Agency; Mark Shelford, Police and Crime Commissioner, Avon and Somerset Police.

Examination of Witnesses

Pete O'Doherty, Rob Jones and Mark Shelford.

The Chair: Good morning and welcome to this evidence session of the Fraud Act 2006 and Digital Fraud Committee. A transcript of the meeting will be taken and published on the committee's website, and you will have the opportunity to make corrections to that transcript where necessary.

We are very grateful to our witnesses for this morning. We have Pete O'Doherty, the assistant commissioner of the City of London Police, Rob Jones, the director-general of the National Economic Crime Centre and threat leadership at the National Crime Agency, and Mark Shelford, the police and crime commissioner for Avon and Somerset, who had himself invited after a very interesting article in the *Financial Times*. I am not sure if that says more about giving interviews to the *Financial Times* or more about what we will hear about your interest in this area. Thank you

all very much for being here. Without further ado, I will ask Lord Young to ask the first question.

Q212 **Lord Young of Cookham:** Good morning and welcome. Can we start off with a general question about the priority that is allocated to fraud by the law enforcement agencies? We have heard from a number of witnesses that economic crime and fraud accounts for some 40% of all crime, but the percentage of police resources allocated to it is a fraction of that.

Perhaps we can start off with a question to Mark Shelford. One of the objectives in the 2011 Act, which sets up the PCCs, is to set the police and crime objectives for your area through a police and crime plan. How would you respond to the allegation that there is an imbalance in all the plans, not just yours, between the incidence of fraud and the resources allocated to it?

Mark Shelford: That is a very fair question. On the positive side, as soon as I took over in the role I wrote to all the other police and crime commissioners with a call to arms to ask them to include fraud and cybercrime as a priority in their police and crime plans. You will be pleased to know—and, in fact, I am delighted to tell you—that every police and crime plan has that as a priority, which is the first time that has ever happened, so we are moving forward.

From the point of view of resources, of course we could do more, but we need to be smarter about how we use the resources that we have, particularly for training and education, and prevention, with the public. I do not know whether I am allowed to give you presents, but afterwards I will give to your clerk, Mark, the postcard that I produced. It is not very expensive, but it goes out to every household in Avon and Somerset with an over-60 year-old, giving them advice on what to do and who to contact if they get into trouble.

Training and police specialisms are an area that we need to work on with all the other agencies to make sure that we are not poaching from each other, that we pay them the right rate and that we train them well. As a quick final example, we train our police officers in a police faculty at the University of the West of England. Next to it is its cyber faculty, but we are not connecting the two and we need to do that better, because that is very simple. We need to change the syllabus to include more digital work and fraud work.

Lord Young of Cookham: That is a very encouraging response. In addition to it being a priority in the plan, are the resources in the plan being reallocated to reflect the growing priority of fraud in the plan?

Mark Shelford: There are more resources going in. Do they reflect 40% of all crime? No. That is an uphill struggle that we are working on.

Lord Young of Cookham: Let me turn to Rob Jones. We have taken evidence calling for fraud to be made a strategic policing requirement and included in the national policing board performance measures. Would you agree with that proposition?

Rob Jones: Yes, I would. Our experience of prioritising threats across serious organised crime has shown that, once you get the threat into crime and policing plans, and it is part of the strategic policing requirement, and if we then, as part of our national leadership, task under the Crime and Courts Act, as we have done with fraud, we shift the dial and it becomes an appropriate priority. I would be supportive of its inclusion in the strategic police requirement.

Lord Young of Cookham: Assistant Commissioner, do you have anything to add on this general issue?

Pete O'Doherty: It is clear that the prioritisation of fraud across policing has not been where it ought to be. Particularly through the spending review, there is a significant investment to build capacity and capability across local, regional and national policing to proactively fight fraud. Is that enough? No, but we are seeing a step change in the prioritisation of fraud across policing.

One last example would be the number of cases that go out from Action Fraud, which is the UK reporting hub for fraud and cybercrime. Police forces and regional collaborations of police forces are now investigating more fraud than ever before, and that is a journey that we need to continue pushing forward.

Lord Young of Cookham: Thank you very much. I am sure that my colleagues will want to follow up on some of the issues that have been raised in those opening remarks.

Q213 **Baroness Henig:** Can I move on to structure? Clearly, the way things are structured is pretty important here. We have heard that there is a siloed approach to fraud, with too much reliance on the City of London Police and Action Fraud, but also an onus on local police forces to investigate cases in their force areas. Do we think that the structure, as we have it at the moment, is effective? If we do not, have we any thoughts on this?

Mark Shelford: From a victim's perspective, the landscape is very confusing. If they ring the local police, the local police will say, "You need to ring Action Fraud". They ring or write to Action Fraud, and they may or may not get a response, so they feel that there is a black hole there. Then, confusingly, it might be allocated from Action Fraud to the regional investigation—the ROCUs—or allocated back to the original force, in my case Avon and Somerset. They find that whole process extremely confusing.

There are other aspects of confusion about charities and investigation of fraud. If a charity has a fraud issue, either perpetrated by the charity itself or on the charity, who is ultimately responsible for that investigation? There is confusion about those aspects.

As far as structure around the agencies is concerned, my only suggestion is that, ultimately, one should be in charge. I am agnostic as to which one it is. I do not mind, but once we know, let us go with that. They are

ultimately in charge, so they delegate out to everybody else. Make it clear to the public that this is the process through which they should put in their concerns, complaints and reports.

Baroness Henig: We have your six priorities set out in information that was sent to us, and fraud is not mentioned. Have you now included it?

Mark Shelford: It is in the police and crime plan.

Baroness Henig: It was not in the material that we got. I know that you have a national Association of Police and Crime Commissioners. Has it discussed fraud and set it as a priority at national level?

Mark Shelford: As I said in my opening remarks, I wrote to all police and crime commissioners right at the beginning of my tour of duty and said, "Please include it in your police and crime plans", and they have done. It is successfully, from a national perspective, in all those plans.

Baroness Henig: But you also have meetings, as a body, with the Home Office. Is fraud mentioned in these meetings?

Mark Shelford: Yes.

Baroness Henig: So it has been discussed.

Mark Shelford: It continues, drip fed, into all the meetings. Is it necessarily at the top of it? No, but is it there? Yes.

Baroness Henig: Can I perhaps turn to Mr O'Doherty for any comments?

Pete O'Doherty: I completely understand how a victim of fraud would struggle to make sense of the current system. I know that from speaking to my own parents, who have been victims of fraud in the past. We need to better explain the system to local communities and to provide absolute clarity about where to report when you have been a victim of a fraud.

We should be evolving the current system, not redesigning it. I say that just because, if you are a member of the public who has been a victim of a fraud, and you walk along your local high street and bump into a local police officer, you should be able to have a conversation with that police officer, who should give you crime prevention and explain where to go to report your fraud and what will happen. There is a role for local policing.

There is also a role for these regional organised crime units, because we have fraud criminals and fraud networks that operate across various jurisdictions, and those regional collaborations are really important for proactively dismantling those operations.

There is a role for City of London Police, because we host Action Fraud and we help policing to improve and build capability. There is a role for the NECC as a system lead that galvanises the efforts of policing, law enforcement or even the private sector to make sure that we are working to common priorities and goals.

To conclude, it is system evolution, not revolution, but we must be better at explaining how the system works in a meaningful way to citizens and businesses.

Baroness Henig: Are you seriously suggesting that 43 police forces should continue, as they are at the moment, to prosecute, in a rather unsatisfactory way, the fraud that may or may not be happening in their area, and then that the City of London has its role? We have had a lot of evidence that this structure is not working.

Pete O'Doherty: With respect, I have to say that the debate on the 43 forces is different, and I have a view on that, of course. My view is that, as long as we have those forces, there is a role and a necessity for the bobby on the street to be clued up about fraud in order to explain it to local people. Whether that bobby is employed by one of 43 forces or one of 10 forces is a different debate, but that local visibility of fraud is essential.

Rob Jones: I recognise the comments about the victim experience, which needs to be simplified and better. On the inherent complexity of a model where you have 43 forces, those points are well made. In terms of our national leadership on the threat, the National Economic Crime Centre has strong legislation in the Crime and Courts Act and convening power to bring together the UK law enforcement response. That needs to operate locally with the volume threat.

What Pete just said is absolutely right. This is mainstream criminality that requires a local policing response, a more sophisticated response in the regions, and a high-end response in terms of capability and capacity with the National Crime Agency and elsewhere. We can transcend those regional and local barriers, and that is why the NCA has the leadership role. We have done a lot to simplify it, and we are doing more, working with City of London, to make sure that we can task work through the system.

I would expect work to come from forces to the regional organised crime units and the National Crime Agency, if it is too complex, and, likewise, work to be driven out from the centre, which is what we are doing. We now have a command and control structure to do that, which is far more effective, and we are seeing some of the results of that.

The Chair: That is very interesting about the command and control structure. Perhaps you can just say a bit more about that and, in particular, with all the different levels, about accountability. Pete O'Doherty might want to comment on that as well, because some of the evidence that we have heard is that, ultimately, lots of people want to help solve fraud, in law enforcement and in other walks of life, but nobody is taking responsibility and accountability for it. We could have in this session all sorts of bodies in front of us, which would have demonstrated just how broadly spread that accountability is.

Rob Jones: That issue exists with serious organised crime across the landscape, and this is a subset of organised crime. The thing about this threat is that there is a volume element to it, which is driven by online activity, amplified by access online. Online is the front line for this, so it does mean that there is not necessarily a geographical nexus for this work and it does require national leadership. We take responsibility for national leadership of that threat with City of London. We need City of London and national policing to drive the local response in communities.

We have wired that together as effectively as we can, and we are working hard to simplify it and do more. From my perspective, through our national strategic tasking mechanism in the NCA, chief officers come to that meeting and, where appropriate, the DG of the NCA issues taskings. We have issued a tasking for fraud and shown leadership in issuing that tasking. A big part of driving that response out is Pete, City of London, the 43 forces and the chiefs who take responsibility for it.

I recognise your description of what we have seen. Where we are now is very different. The operational effect generated from that needs to be higher volume and more impactive, and we need to see more action, but the structure is significantly better than it was.

The Chair: When was that tasking issued? When did that really take off?

Rob Jones: We can provide details of the tasking, but as an example of the type of thing it drives, in March of this year, through national policing, we co-ordinated an intensification against fraud, where 364 cease and desist notices were issued. Over 300 people were interviewed under caution in one month. Our plan is to run that type of intensification quarterly against this threat, with national policing, against the volume, while we go after high-value targets and more complex operations.

The Chair: We have plenty of other questions, but I do not know whether there is anything that you want to add on the tasking structure.

Pete O'Doherty: No, we just echo the points from Rob Jones.

The Chair: Mr Shelford, I was interested in your election campaign. Did fraud come up much when you were talking to the voters?

Mark Shelford: It did, which is why I volunteered to do the task. I was lucky or unlucky enough to have two and a quarter years as a candidate, because of Covid. I must say that I was not delighted when I got the phone call that it was going to be delayed a year, but it gave me the opportunity to go round and knock on a hell of a lot more doors and, when I could not knock on doors because of Covid, to phone people in the afternoon.

I was struck by two things: first, the sheer volume of people who mentioned some form of fraud, phishing attack or scam that they had suffered; secondly, Citizens Advice, which reached out to me on a number of occasions and was utterly swamped by the number of people who had asked for its help. So the short answer is yes.

Q214 **Viscount Colville of Culross:** Good morning. Mr Jones, we have just heard how the enforcement agencies are training and working together to make sure that there is enough expertise to deal with fraud, but do you still think there should be a clear strategy for funding the right skills and making sure that they are in the right places to deal with this problem?

Rob Jones: Yes, absolutely. To get people who are digitally aware and are digital natives, and to turn them into law enforcement professionals, is challenging for a number of reasons, some of which I will go into.

First, it takes 18 months to two years to grow one of those individuals. From that level of investment, once it is delivered, our payback is immediately at risk. They are a flight risk, because as soon as they qualify they can get a life-changing salary offer from outside industry. If you are particularly good at cyber or fraud, you can, in essence, double your money at the entry level for our grading structure. You have to want more than money to work in the public sector, so that is a fact. It is not just about money, but it is about a reward package that is attractive enough to retain people and to recruit them in the first place.

The second point is capacity in the system. Mark has already said this. We do not want to be competing in the law enforcement system for the same individuals. The Cabinet Office needs counter-fraud professionals. The NCA needs people with those skills who have law enforcement powers. City needs them; the 43 forces need them. We need one solution and one strategy that creates a pipeline of people who can do digital investigation at varying levels of complexity.

I will return to what I said earlier. This needs to be mainstream, local policing, so that digital investigation is no longer a specialism; it is the world we live in. If you turn out for burglary or assault, you need to have the same level of training in the digital world to cope with what you find.

Create a pipeline that is based around a profession, and have enough resilience in that pipeline, so that when there are challenges of investment or demand, you can access that pipeline, but it needs to be a multiyear pipeline that pulls people through. If we do lose people to industry, great, they can go away and perhaps come back in the future, but we have enough resilience in that pool to bring it forward.

Viscount Colville of Culross: Who would be in charge of this strategy for recruitment and retainment of these digital operatives?

Rob Jones: There are a range of solutions that are in play at the moment, which probably need to come together. The College of Policing is part of the solution. We have our own investigation training programme in the NCA for graduate entrants and apprenticeships. We also have a programme around specials to allow people who are not full-time law enforcement officers to make a difference. We do not yet have enough to satisfy the demand across the systems, because police uplift, the ROCU uplift, NCA growth and our aspiration to grow are all challenged by our ability to bring people through quickly enough.

Viscount Colville of Culross: Assistant Commissioner O'Doherty, there has been a call for the economic crime delivery board to commission a review into the disparities in skills between the private and the public sectors. I imagine that you support that completely, but is there any possibility of ever being able to match the extraordinary salaries? Mr Jones has talked about the glories of public service, which we here all understand, but, in the ruthless world of digital skills, that is pretty hard to enforce.

Pete O'Doherty: From a financial point of view, I do not see completely matching industry salaries as a solution or a realistic outcome, but we should certainly offer more, in the ways that Rob described, than we currently do. It is not just about remuneration, but about accreditation, training and support. We need to diversify the way we attract and recruit people into policing, for example, so targeting colleges and universities.

In fact, I spoke to Rob and Mark yesterday, and Rob had a really good idea. Say we know that this really great graduate in cybersecurity is looking for a job in industry in five years. If they get the job in industry, we could provide the training in law enforcement. They give two or three years' return service and then they begin their role in industry. That is great for industry, because they are fully trained, they have police and threat experience, and they have work and life experience. Equally, we get five years from that person, so there are different things that we could do.

We are doing lots of work around leveraging and mobilising volunteers and specials. At the moment, across the UK, we have cyber resilience centres, which give cybercrime prevention advice, to SMEs in the main. We recruit students half way through university degrees to provide cyber products to businesses, which cost about 50% less than the market rate. They are very attractive; they get work experience and, for me, that is a great example of a recruitment pool that we should be targeting into policing.

For fraud and cyber, we are creating an app for anywhere in policing where you want a specific skill. Let us say that you want someone from industry who does Python coding or scripting, or an expert in cybersecurity. You can put the skill set that you want in the app, and it will connect you to a special constable or volunteer who works in the police from industry and who has that skill set, so that we can leverage that capability in that way.

We have some people from industry already working in our department. Microsoft sits in our intelligence department and looks at all the computer service software frauds that come into our department. This is traditionally a contact centre that phones you to say, "Your Windows platform is out of date. We're going to give you a free upgrade". It has remote access to your machine. It does the free upgrade, but what it has really done is deployed a virus into your machine, and it watches you inputting your address, username and password for online banking.

Microsoft looks at those crimes coming into our system. It looks at how

its platform could be updated to prevent that crime happening in the future, and it takes that learning back into Microsoft.

In conclusion, there is no one simple answer. Improving the response to fraud is not just about having more people, but about mobilising industry, working differently. As well as targeting young people to work in policing and law enforcement, what about people retiring who have been detectives for 30 years? They might not be digital natives, but they have the accreditation and the experience. We just need to be really broad and diverse in the way that we address this challenge.

Viscount Colville of Culross: That is extremely interesting. You have given the Microsoft example. Is that just your idea that should be rolled out further to get that relationship between the enforcement agencies and industry? It is a no-brainer. How can you get that rolled out much further?

Pete O'Doherty: I am sure that Rob will have some comments, but we have a few examples. We are trying now to industrialise that and make it much larger scale. The introduction of the online harms Bill will provide new opportunities for doing that at a much larger scale. I know that Rob and the system leadership are doing lots of work in this area as well.

Rob Jones: We have a public-private partnerships team in the National Economic Crime Centre, which reaches out to industry. The National Cyber Crime Unit, which is part of my command, has a really strong relationship with industry. The insight that we get from industry is key to us tackling the threat. All the people you would expect are represented there. There is some really good work there and that is a very strong example of the difference that can be made.

Mark Shelford: Locally, that story is not the same. We are utterly failing locally to attract those experts. We cannot even recruit straightforward IT experts at the moment. We will probably have to go to an agency to do our support and regionalise it to try to attract them. We are being creative, though, and we are not wringing our hands. The business about specials, recruiting part-timers and working with the military reserve in certain areas is something that we are doing right now, but it does not make up for the ability to recruit and retain specialists in those areas.

Viscount Colville of Culross: You have some of leading universities in the West Country. Are you working with Bristol? You mentioned the University of the West of England, where you are now, but is that not an obvious place to go to try to recruit?

Mark Shelford: We are. There is an element of that direct approach, but also an element of the College of Policing and freeing up the syllabus to give us more space to do that. We are being creative in trying to get round these problems, but it is not simple, it is not easy and we do not have a solution yet.

Lord Vaux of Harrowden: You have talked about the recruitment of people into the police and about working alongside industry, but one of

the ways in which you can avoid or solve the problem of the private sector competing for people is to employ the private sector. There are many companies out there that are real experts in data analytics and all the things that you need to do in fraud. To what extent do you contract the private sector to work alongside you, as opposed to the Microsoft arrangement, to do this?

Mark Shelford: We are now looking at doing exactly that, because we have failed to recruit. We have just started that process.

Rob Jones: We contract the private sector to tackle both cyber and fraud, because there is a very rich vein of talent and data there, but we need skills transferral and we need to grow our own. As for being able to access industry, yes, I absolutely agree, but there needs to be a balance, because what this whole threat area—dealing with all online threats—has suffered from is not investing, digging in and creating digital skills in law enforcement. That needs addressing, which means that we need to focus on growing our own talent as well as accessing other areas for support.

Pete O'Doherty: In the City, we have had two investigation teams completely funded by the private sector. One is the card and plastic crime unit, which has been going for 20 years. We have an insurance investigation department funded by the insurers. They have embeds from those organisations working with our cops, analysing threats and leading on investigations.

We also have the industry embedded in our intelligence department. Microsoft is the example that I gave earlier on. We use the private sector in many ways, whether it is designing a new technology platform or helping us in communication and prevention messages out to businesses. We work with the private sector very proactively, but there is more work to be done, of course.

Q215 **Lord Sandhurst:** This question is directed primarily at Rob Jones, but also probably at Pete O'Doherty. I do not mind if Mark Shelford has an answer as well. Rob Jones, you told us about your aspirations and how you are trying to develop various things. Is there an actual programme in your organisation? If you were to come before this or a similar committee next June, first, what would you be telling us that you now have in place and are doing that you do not have at the moment? Secondly, do you have the funding for that? Thirdly, if there was a way of levying fines or compensation requirements on the platforms, would that boost your resources?

Rob Jones: On your first point, across the SR period there is a plan, which is building capability and a national fraud network with City of London and others, with some significant investment. Over the next three years of the SR period, that gets us so far, but the aspiration, working with the Home Office, is for a 10-year strategy that really deals with this. The here and now means that we need to work very quickly to develop and drop that capability in, which is what we are working to do. That plan is there.

On the point about funding, it is funded, but that is set against the context of us, at the same time as planning that growth, also modelling for potential cuts to the size of the agency as part of the Civil Service reforms. I am heartened by some of the remarks that were made yesterday about the agency, and the agency not being cut, but, at the same time, we are civil servants. That gives us a very flexible approach to employment, but it also brings us into the purview of modelling those cuts. I say "modelling", because those cuts have not been made, so we are still planning for growth and pushing hard to develop that network.

Lord Sandhurst: It is along the lines of the SEC in America, which takes a slice of the action.

Rob Jones: Absolutely, yes. With the plans for the economic crime levy, there will be benefit to the system from that. That benefit will be broad and will impact on fraud as well. The potential for fines on platforms and what Ofcom may do as part of the regulation under online harms is another area where you could generate funding. There needs to be zero tolerance online by platforms that host some of the materials that allow fraud to be perpetrated, and it feels right that there should be some benefit from the system if there is a dividend from fines.

Pete O'Doherty: A year from now, as a very minimum, we want to deliver the following, to give you a few examples. One is a new reporting platform for Action Fraud.

The Chair: We will come on to that in a moment, so do not say any more.

Pete O'Doherty: No problem—please just stop me if these examples are going to come up later. We want to deliver nine proactive fraud investigation teams across the UK, proactively dismantling fraudsters; a people strategy complete for that big uplift across policing; more intensification periods in fraud, like Rob described before, with hundreds of people arrested and millions of pounds distrained; lastly, the rollout of our economic crime victim care unit, which provides services to victims of fraud across the entire country.

Lord Sandhurst: Does the money distrained go into the general pot at the Treasury or can you get a percentage of it?

Pete O'Doherty: We get a percentage. It depends on the mechanism for the asset restraint, but, invariably, we get a slice of that. We then invest in improving the provision of local services to local communities.

Q216 **Lord Vaux of Harrowden:** You touched on Action Fraud, which we are coming back to. I was interested in that last list. You did not mention reducing the levels of fraud, which I think is a target that should be there, but, anyway, that is a separate question.

We have heard already from you about the shortcomings of Action Fraud as far as victims are concerned. The words "Inaction Fraud" are often used to describe it. More generally, we have had a witness who tells us

that it has become a useful veil from which the police hide their inadequate response and that it has irretrievably lost the confidence of the public.

Government has announced plans to replace it and, more recently, has mentioned that it is working with City of London Police to upgrade Action Fraud, which is slightly different from replacing it. Perhaps Pete O'Doherty could explain what is happening with Action Fraud and what you expect the end state and the benefits of that to be.

Pete O'Doherty: I am mindful of time, because I could speak about this for hours, but I will not.

The Chair: If there is anything written down that you want to refer us to, or if you want to write to us, you are always very welcome to do that.

Pete O'Doherty: That would be great. Thank you so much, Chair. In brief, there are two reasons why there is that rightful perception of "Inaction Fraud", and I get it. The first reason is that, no matter how good or accessible Action Fraud is, or how good the technology is in the customer journey, as long as we are not investigating fraud, there will always be the inaction in Action Fraud. Action Fraud is the front door into our response to victims, but all the work that we have been discussing will, I hope, improve that.

The second issue is the technology, which we are addressing through this procurement. If you report to Action Fraud, we are not great at telling the victim what will happen or is happening. In many cases, a victim does not get an investigation from policing, and we need to be better at explaining why. For 2024, we are implementing a completely new infrastructure for Action Fraud and the National Fraud Intelligence Bureau, which receives the crimes that go into Action Fraud, which then determines what cases go out locally, regionally and nationally, across law enforcement, for investigation.

In short, what can we expect that will be different? First of all, when you report your fraud to Action Fraud, it will have a new function called "track my crime", so you can log on to the dashboard and it will explain to you exactly where your fraud is in the system. If it has not gone out for investigation, it will tell victims absolutely why, but reassure them to say that we will be using the intelligence that we have around that case to do some other proactive work. That is one example of what it will do.

It will have automation. For example, at the moment, it takes us a little while, on occasion, to get some cases out to policing for investigation. By the time a police force receives an investigation, if it is four or eight weeks old, the suspect is long gone and there is very little that a police force can do. With better automation and the linking of cases, we will get cases out much more quickly to policing, so that they can identify and arrest suspects, which is a good news story for victims.

It will have a new website that is more informative, which looks at the crime you are saying has happened to you and immediately, using AI, pushes crime prevention advice to you to say, "Look, the next time you

use a dating website, these are the things that you need to check before you engage with a person who purports to be a soldier in America looking for love". Using automation, it will understand how victims are being targeted and, using that learning, it will produce better prevention advice that is automatically sent out to victims to prevent repeat victimisation.

These are the kinds of big benefits that the new system will have. We know that the people who commit fraud are also committing other crime—human trafficking, drugs importation and firearms. Action Fraud needs to link those cases together better in order to make it easier for policing to say, "Well, look, we know that this person is involved in fraud and in human trafficking", so we can have a co-ordinated response to investigating this person and joining up the dots more.

These are some of the benefits that we will see. Lastly, going live this year is a 24/7 cyber reporting service for victims. The call handlers you speak to are specifically trained in cyber. As a business, particularly an SME, you do not really know how the ransomware happened or what to do next. That contact handler will walk you through the process and help you to report your crime.

I would absolutely welcome, Chair and my Lord, an action to write to you with some more information around the improvement and evolution of Action Fraud.

The Chair: Thank you. That would be very helpful.

Lord Vaux of Harrowden: That would be great. Mark Shelford, from your position, what do you want to see from Action Fraud? Is it what we have just heard, or are there other things that you think we should be looking for?

Mark Shelford: I must declare an interest, because I am on the board, so I see this as part of the development. The biggest single issue is that feedback to victims. It is so important, because just going into a black hole, which sometimes happens now, is really emotionally destabilising for people.

The other aspect, absolutely, is that automatic prevention piece, which is really important in order to prevent them becoming victims again. A better explanation of the thresholds that then drive investigations is important, because it is very difficult, particularly if you are a new victim who has just had your life savings stolen. How on earth do you put that together in a very few words that show that a crime has been committed and will result in an investigation? It is difficult, even when you are not emotionally involved in it, so understanding what those thresholds are to tick the box to get an investigation is very important.

Lord Vaux of Harrowden: Rob Jones, from the other side of the equation, we have talked about Action Fraud from the victim's point of view, but it also has to be helpful and useful to the police forces and the crime processes. Do you see it doing that, and are there other things that we need to do?

Rob Jones: Yes, absolutely. We work very closely with the programme to make sure that we have a very powerful data exploitation capability. The opportunity for us is a new system with new technology that will allow us to get to that data much more effectively and join the dots. We can be proactive and identify organised crime networks, deal with those as a crime in action, and disrupt them before they victimise people. That is one of the big dividends that we hope to get from the new capabilities that Pete has described, and we are working closely to make sure that it will plug into the NCA capabilities.

Q217 **Lord Gilbert of Panteg:** Thank you for the evidence so far. You have reinforced an issue that has become clear as the inquiry has progressed, which is that it is not at all clear to us who is in charge of policy in relation to preventing fraud. You have described the confusion at a policing level and for victims, but it seems to me that there is a wider issue, which is that there is a lot of a confusion about who is in charge of policy at government level and which bodies are in charge of bringing industry, police and government together. I just wonder whether you can reflect on that and describe to us what co-ordination you think is and is not working, and whether there are too many bodies trying to do the same thing.

I would also like you each to tell me which government department and which Minister you think is in charge of counter-fraud policy.

Rob Jones: As the NCA, we work very closely with the Security Minister and with the Home Secretary in relation to this as a serious organised crime threat. With City of London, we are regularly updating the Security Minister on our law enforcement efforts to tackle fraud; there is very clear leadership there. The officials who work with the Security Minister and the Home Secretary are our interlocutors in the NCA efforts to do that and there is a clear line of sight there. I have to say that they have been very supportive in planning to increase capacity and capability.

That said, as with all crime and serious organised crime issues, there are a number of other interests out there. That crystallises with online harms, because DCMS and other departments have a strong and legitimate interest in what takes place. As ever, across Whitehall, bringing together those interests to an apex so that we have some clear leadership is a challenge, but from where I sit there is clear direction from the Security Minister and the Home Secretary about what we need to do. That is where we turn to officials for policy leadership.

Lord Gilbert of Panteg: Is it clear who represents business—banks, telcos and platforms? You have all talked about a number of programmes with different businesses. Is it clear who represents those key business groups right across the piece?

Rob Jones: In the regulated financial sector, UK Finance is a really strong partner. We work very closely with it in the NECC and in a number of groups. It comes to the ministerial groups that are tackling these issues. On tech sector issues, we have worked with techUK and we have

an online fraud steering group, which was set up to bring those interests together.

The challenge with that sector is that it is not regulated and the balance of power is on the west coast. That is very well rehearsed, which is why we have the Bill coming through and why we need a regulated environment, because an unregulated internet is a failed experiment, in my view. That is more challenging, but through techUK, DCMS, the Home Office and work on the Bill, that has been pulled together. Where you do not have regulation, it will be disparate and more ambiguous, so regulation cannot come soon enough for us in that space.

Lord Gilbert of Panteg: Mark, you talked at the start of this session about confusion, primarily for victims of crime, but, as I say, it extends a bit further. You are a military man. You come from a military background and have a distinguished military record. You must be used to clear command structures and objectives. Do you see that generally increasing, very specifically in this war on fraud? Are there lessons that we could draw from the military and your particular experience?

Mark Shelford: That is a marvellous question and I do not have a simple answer to it. It can be improved significantly, as I said at the beginning. There is confusion out there for the victims, but there is also confusion about policy. I am open to all sorts of organisations and Ministers suggesting ways of improving how we support the victim, but also how we prevent this crime.

A golden thread through my police and crime plan, which I would recommend to all of you as a good bedtime read, is prevention. That is in all crime, but particularly fraud. It is so much better if we are stronger and educated and we can stop the crime happening before it penetrates into our homes, our houses and our families. There is confusion out there, and I do not think there is a straight chain of command.

Lord Gilbert of Panteg: Do you think that a lack of command structure partly contributes to that?

Mark Shelford: I do, yes.

Lord Gilbert of Panteg: Is that from the top—from government, through policing, prevention and education?

Mark Shelford: Yes.

Lord Gilbert of Panteg: Pete, what are your thoughts? You are very focused on the policing aspect of it, but you work with a range of other agencies that you have already described. How joined up do you really think it all is?

Pete O'Doherty: It is well joined up. All the questions and issues you describe are being addressed and discussed through the fraud reform programme being led by the Home Office, which is the beginning of the 10-year fraud strategy delivery. All the questions around mobilising the

private sector, leadership around fraud prevention and campaigns are in scope of fraud reform programme that Rob and I are firmly involved in.

On the discussion about command and control, I do not have a distinguished military background, but I would say that when there is an active fraud threat, command and control is essential, and between us, under the NECC as a system leader, works really well. Some of these issues that we are discussing are wicked problems. They are strategic issues that require agencies and organisations to be empowered, creative and innovative. If you have a command and control approach to addressing those wicked issues, I fear it might stifle innovation.

For me, it is easy to say that the system makes sense, because I am in it and live in it every day. We need to make it clear and give it sense to an outside victim—an elderly victim not connected to the internet—in order to help them to understand, navigate and make sense of the system. That is what our efforts need to be focused on.

Lord Gilbert of Panteg: If you came back to us in a year's time, how different do you think it would look? You have described the work that is under way to bring all these functions more closely together and to co-ordinate them more effectively. What will that look like in a year's time? I fear we will just have another bunch of acronyms on top of all the others that we already have, and another couple of bodies duplicating stuff that is happening elsewhere. Do you think lots of these streams of activity will have been swept up and brought into one structure, certainly at policymaking level?

Pete O'Doherty: A year from now, we will have the 10-year fraud strategy published. We will have the completion of the fraud reform programme. We will have a sizable investment across the National Crime Agency and policing in preventing and investigating more fraud. We will have a clarification of the system governance around the delivery of fraud prevention and enforcement activity, because that is in scope of the fraud reform programme. We will be a year closer to a new Action Fraud system. I am confident that, a year from now, although we will not be at the end of the journey, there will be no new layers of governance, no new organisations, and certainly more momentum in our delivery.

Lord Gilbert of Panteg: Great, I look forward to talking to you in a year's time.

The Chair: Rob Jones, we talked about online platforms and about the banks and UK Finance. What about the telecoms companies? They are critical, are they not, in delivery or facilitation of fraud?

Rob Jones: Absolutely, yes, and it is one of the examples where we are seeing positive change. We have had some very recent success as a result of Ofcom working with the telcos, because they are regulated and they have a footprint here. That has allowed a significant impact on malicious SMSs, which are sent out promiscuously and generate fraud.

Some of those operators have seen over a 70% reduction in that traffic on their networks by engaging in technical activity, which, I would summarise, is a technical defence to prevent those messages meeting customers. There is some really strong work there, which is being developed further through the online fraud steering group. They have responded, and have responded well, and we have seen the dial moved on that threat vector to victims.

The Chair: It is quite recent.

Rob Jones: It is, and it is a direct result of this level of prioritisation and challenge to industry.

Q218 **Lord Sandhurst:** These questions are directed primarily at Pete and are about Action Fraud. In the last year, the fraud advisory panel found that at least 61,000 crime reports to Action Fraud cited social media. Much more recently, Lloyds Bank research has found, first, that WhatsApp scams have surged in the year by 2,000%, whatever that means. These are impersonation frauds and they are on the up.

Secondly, 70% of investment frauds reported to TSB started on Facebook or Instagram, so specific platforms. That is the context. We will take the questions in stages. The first one is whether Action Fraud keeps a record of the names of platforms or companies most cited in reports of fraud.

Pete O'Doherty: Yes, it does.

Lord Sandhurst: Good. Are you prepared to share those details with the committee?

Pete O'Doherty: Given the acute awareness of the use of social media in fraud and social engineering, and particularly given that all the platforms I could speak to you about would be no surprise, I am more than happy to share that.

Lord Sandhurst: My understanding is that, at the moment, Action Fraud does not publicly name and shame particular companies. Looking forward, would it be helpful if you could work with, say, Ofcom or the CMA to insist that the various platforms and intermediaries—I am thinking particularly here of the ones we have looked at: Facebook, Instagram and WhatsApp or similar—inserted on these platforms great big warnings or advertisements? They would have to offer you the right to do that for free, and that would be a regulatory requirement—in other words, public information to young people or anyone using any of these platforms. I do not know whether it involves TikTok, but certainly the others have all been named. They should be able to take public advice from you so that users get it.

Pete O'Doherty: Even though I would always say to you that these social media giants need to do more, they are, on a day-to-day basis, very supportive of the work we are doing. If we have a specific investigation, they work with us closely. Interestingly, to your point about displaying that warning message—"There's illegitimate advertising in your business and we've taken it down"—we already do that on websites. If a

website is operating illegitimately, we will remove that platform by working with partners and put up a sign saying, "This was an illegitimate website. This domain no longer exists and we've taken it down for these reasons".

I have to say that what we have been missing is the very framework that you have described. The online harms Bill, which I mentioned, will now give us that strategic provision to really have that conversation with those social media platforms in order to get them more committed to prevention at scale.

Lord Sandhurst: If, say, Ofcom were to beef up its regulations to say, "Our requirement in the UK is that WhatsApp"—or whoever it is—"offers Action Fraud the ability to insert warnings or adverts and, if you do not offer that on a decent basis, you will not be allowed to operate", would that be helpful?

Pete O'Doherty: I would hugely welcome that, or anything that helps prevent victimisation, which I am committed to, 100%.

Viscount Colville of Culross: Pete, just picking up on the Online Safety Bill, you said that the clauses about stopping fraudulent advertising will be very helpful. We have been told that the search engines have a much diminished responsibility. If it is about prevention, would it not be helpful if the platforms, rather than helping you after the fraud had happened, were part of the prevention activity? There is already this safety by design for all sorts of other harms taking place. In your world, where one of the greatest harms is taking place, should more be done to encourage a duty of care by the big platforms, certainly in category one, to try to prevent fraud happening on their sites?

Pete O'Doherty: Absolutely, yes, and I really hope that between now and the harms Bill receiving Royal Assent, those companies and search engines know that that is coming and will start to work with us on that prevention piece. It is important to protect victims, and it will make their life much easier, as opposed to being held to account after the fact. Through the online fraud steering group, techUK, UK Finance and other partners, we are starting to have these discussions now.

The Chair: Rob Jones and Pete O'Doherty in particular are being very polite about the platforms and their working together. We know that there are variable standards and willingness to work. You might not want to publicly name and shame here, but we know of at least one large retailer that, so far, is refusing to give oral evidence to this Committee. It is Amazon; that is public knowledge. I have written to it publicly. If you wanted to tell us, either here or separately, of any platforms that are particularly dragging their feet or anybody who has been very slow to come to work with you, that would be helpful.

Rob Jones: As a brief comment on that, we are disappointed if we see a big player like that not coming to speak openly about this. We are also surprised, because they have a strong capability and we work closely with

them. On a case-by-case, episodic basis, they are positive and will work with us, just as Pete described.

The real challenge strategically is the proactive detection and prevention of fraud and that duty of care, and the balance of power on that really sits on the west coast. That is where we need to extend our reach extraterritorially to say, "This is an existential threat to your business model unless you change". Until that happens, we will not make the move from chasing operation by operation to seeing a big preventive shift online. That is part of the challenge around the legislation that is coming through.

We may be being polite. We are being accurate about our relationship with individuals, but the fact is that, strategically, WhatsApp has been end-to-end encrypted since 2014. If WhatsApp wanted to go after content that is fraudulent on that platform, it could not do it, because it has locked itself out of its own content. That is the type of big strategic challenge that we are addressing here.

The Chair: Thank you. We now turn to victims and consumers.

Q219 **Lord Allan of Hallam:** I want to come back to something that we have already covered at various points during the hearing, which is the experience of people particularly in contacting Action Fraud. We have taken evidence of the difficulty that people have in reporting and following up on cases. Pete O'Doherty, you have indicated to us that you will put in place a new system that should improve matters with case tracking et cetera. Are you, today, evaluating how people feel about the effectiveness of the service, and do you have a plan to evaluate the new system, so that we can compare before and after?

Pete O'Doherty: We do, in two ways. First, we survey people who report initially to Action Fraud around accessibility of the reporting service, but as you can imagine it is very biased, because they have not been told at that point that they are not going to get an investigation. The satisfaction is very high at that point and, as you can imagine, it drops as it goes through the service.

Secondly, we have an economic crime victim care unit, which provides level 1 and level 2 services. A level 1 service is for a non-vulnerable victim. We will write to a victim and say, "We see that you've been a victim of a fraud. We're really sorry that's happened. This is the process. In the future, do X, Y and Z to protect yourself".

We then have a level 2 service, which is for vulnerable victims. That is a phone call and a really detailed discussion about their finances and crime prevention. We will survey the people who receive the level 1 and level 2 services to help us improve in the future. We are quite proactive around feedback to help shape future service provision.

Lord Allan of Hallam: Do you do that by demographics? I can imagine that your tracking service, for example, will be fine for people who like going to websites. There will be other people for whom that will be a

challenge.

Pete O'Doherty: Absolutely, yes. As you can imagine, our vulnerable victims tend to be elderly people and people not connected to the online space. We make sure that the provision of victim care is bespoke to the needs of that individual. Some of the people we speak to have mental health challenges. One of the challenges we have is trying to mobilise social services to provide additional support to those people.

The other complexity is that some reporting to Action Fraud is third-party reporting—for example, for a person who is very elderly or not confident in using a telephone or the online reporting tool—so how do we deliver that prevention advice through the third party to the person they represent? There are all these complexities. On average, we reach over 7,500 people every month for both the level 1 and level 2 services.

Lord Allan of Hallam: Mark Shelford, I am curious how confident you are that the ordinary victim in Bath and Bristol will benefit from the changes that are being made to the national Action Fraud service and this crucial link to somebody who can go to the house of that individual victim. I assume that you need to negotiate that with local authorities in your area. Does that work well, or could it be improved?

Mark Shelford: I am confident that the improvements will make a significant difference to the people in God's own County of Somerset and Avon. Beyond that, we currently have officers who look after victims in the fraud arena. They go and support those people who have suffered from fraud, particularly in trying to make sure that they do not become repeat victims. That could be romance fraud or investment fraud. We had a very significant money flipping fraud in Bristol that used Instagram to spread the message.

I am confident that we will see an improvement. We are working well with the City of London Police and the NSA, but there is more work to be done on this. We are helping ourselves as well.

The Chair: The draft victims Bill has just been published. Does Mr Shelford or the Assistant Commissioner have anything to say about whether that will also make a difference to those they look after?

Mark Shelford: As part of that, greater responsibility is outlined for PCCs, particularly from the point of view of the local criminal justice board, of which I am the chair, to make sure that this is part of those priorities. Indeed, it is a priority in my own criminal justice board, and we are working through what that means in practice.

It is really important to understand that there is a change of emphasis. It is not just the financial effect of these frauds; it is also the emotional effect. That had not really been thought about previously. Some of these are utterly devastating. I met some people the other day who had suffered from romance fraud. They were incredibly embarrassed about it. They could not tell their families about it and, as a consequence, they

were laying themselves open to this happening to them again because they were not seeking the right advice or help. We need to get the message out about that.

This postcard, which I hope you will get afterwards, is specifically for grown-ups to put next to their phones, because they are more likely to have landline phones. They can stick it on a wall. It just gives them a few clues about what to do if they feel that they are under threat.

Pete O'Doherty: We are very well engaged with the Bill and welcome it. It will make a big difference to victim care. There are only two issues. First, it does not mention victims of economic crime specifically. To Mark's point, specific victim care is required. Secondly, there are thousands of business victims. How do we provide improved victim care to businesses when, of course, one fraud could put an SME out of business for ever? Otherwise, the feedback has been welcome and received.

Q220 **Baroness Bowles of Berkhamsted:** This is really a question to Rob Jones. I would like to probe a little more about messaging and campaigns. We understand that the NCA is currently undertaking a review of those things. Can you provide an update on that review and your learnings to date?

Rob Jones: We have done a significant amount of work in relation to how we can get messages to the public. We have used this term in the past of "breaking the spell" between victims and fraudsters. The playbook that is used by a lot of fraudsters is very similar to online grooming that we see elsewhere. You need trusted sources of information so that people, as Mark and Peter described, can recognise what they see in front of them quickly.

We did some initial polling, which indicated that 80% of the group that we polled was not aware of 11 out of the 13 communication channels that provide counter-fraud advice and messaging. There is a challenge there. The next stage in that work with the Home Office is to strategically look at how we can channel people to those trusted sources of information as quickly as possible, and amplify and intensify those comms to create resilience in victims.

There are a number of places you can get advice and some really strong messages out there in Cyber Aware and Take Five. There are a number of them, and a number of them are unknown by large swathes of the public. The next stage is to squeeze that and to channel people as best we can to those trusted sources of information. There is clearly more work to do. It is a really important part of what we can do to create resilience in victims.

Baroness Bowles of Berkhamsted: We were told by the FCA, for example, that having some kind of central body with allocated funding would be more effective in terms of both the messages it could deliver and getting more bang for your buck money-wise. Is that part of it?

Rob Jones: That is a potential option. There is a view in the community that that may work, but there is also something to be said for a diverse number of channels to deliver to the broadest possible audience. That work is more likely to be evolution than revolution, in terms of us being distracted by trying to kill all these channels and their comms and get them into one central place. The next stage is about channelling people to trusted sources of information really quickly. That is what that work will do. That does not necessarily involve having one body that does it all.

Baroness Bowles of Berkhamsted: Might you not be missing out? A lot can be done utilising behavioural sciences and all that kind of thing, and that costs if you are going to access it. Should that not have a central access point so that it can be distributed rather than the same work being repeated? I agree that it can be tailored by other organisations, but there must be some that it is better for everybody to have access to and to reinforce messages on.

Rob Jones: No, I agree, and that option will form part of the consideration as we take them forward. I recognise and agree with the point you are making about the economies of scale and the support from behavioural science, nudge and a whole range of ways of getting people to do the right thing and make the best decisions. Yes, it is an option that I am sure will be explored.

Lord Vaux of Harrowden: To what extent to you get involved in campaigns with schools and universities, particularly universities, on money laundering and muling, et cetera?

Rob Jones: We have done some campaign work in academic institutions, particularly on cyber-enabled fraud and money laundering. That is a really good example. Yes, we have done it and it has been productive. The challenge for the comms piece is that there are strong products with operational insight, but market penetration and ways to get them to the right people are lacking. The delivery mechanism for that messaging is really important to us. We are working closely with the City of London and others on that. That is a very good example around money muling of something that worked well when we went out on campus.

Q221 **The Chair:** The final question is whether you have one particular policy recommendation. We have covered a lot of ground and lots of things that perhaps need to change or be enhanced. If there were one recommendation you would want us to see us putting in our report as a committee, what would it be?

Mark Shelford: It would be a carrot and stick approach to the platforms. The carrot is working well right now, but the stick approach would be to consider revising current corporate criminal liability to include a new failure to prevent offences of economic crime, including money laundering and fraud.

The Chair: I had not planned to have a follow-up on one recommendation, but you might want to write to us. Of course, the Law

Commission came out with its proposals on failure to prevent last week. I do not know whether you have any quick reaction on that. Alternatively, you are very welcome to write to us.

Mark Shelford: I have rather more asks, so I would be delighted to write to you.

The Chair: We will look forward to hearing you on that. Thank you very much.

Pete O'Doherty: To address and solve these problems, we need to think about not just next year, but in the next 10 years. I know it will not be the first time that a police officer or public service department has asked for more money, but I would say that the investment, which is good at the moment, needs to be sustained over the long term. If we are producing a 10-year fraud strategy, I know we cannot expect detail, but we need a longer-term commitment on investment to help to do the work on prevention, enforcement and mobilising the private sector. A long-term investment strategy would be my recommendation.

Rob Jones: I support the points that have been made. There are perhaps two points. One is the enablers for fraud. We all have laser-like focus on arresting people, kicking doors in and getting after bad people, but the really big dividend with something of this scale is when you impact on the offending environment. We need to be very sharp and have a different risk appetite for doing things without changes in primary legislation.

I would call out the faster payments system as one of those areas that we need to look at. You do not want to disrupt a wonderful system that everybody relies on or to disrupt access to banking services, but for the small subset in all those faster payment movements that is fraudulent, if you slowed it down you would do a lot of good. If you slow it down, engage a cognitive response from the victims and get them trusted information, they will not send their money to the wrong account. Authorised payment fraud absolutely cries out for a second look. We need to challenge ourselves as a group and a system as to why we cannot do that right now.

The Chair: That is incredibly helpful. Can I thank you all very much indeed for your time this morning? I know that some people enjoy giving evidence to Select Committees, but it is something some people would rather not be doing. It takes time to prepare for, but we are really grateful. You have been very generous with your time and your evidence. There will be follow-up, so we will obviously follow up with you and your teams.