HOUSE OF COMMONS

Justice Committee

Oral evidence: Fraud and the Justice System, HC 961

Tuesday 22 February 2022

Ordered by the House of Commons to be published on 22 February 2022.

Watch the meeting

Members present: Sir Robert Neill (Chair); Ms Diane Abbott; Rob Butler; Angela Crawley; Laura Farris; Paul Maynard; Dr Kieran Mullan.

Questions 1 - 62

Witnesses

I: Mike Haley, Chief Executive Officer at CIFAS, the UK's Fraud Prevention Community; Dame Vera Baird, Victims' Commissioner for England and Wales; and Wayne Stevens, National Fraud Lead at Victim Support.

II: Temporary Commander Clinton Blackburn, Head of City of London Police's Economic Crime Directorate; Rob Jones, Interim Director General of the National Economic Crime Centre; and Mark Shelford, Police and Crime Commissioner for Avon and Somerset and Economic and Cybercrime Lead of the Association of Police and Crime Commissioners.

Written evidence from witnesses:

– Association of Police and Crime Commissioners

– CIFAS

– The Victims' Commissioner for England and Wales

– Victim Support

– City of London Police

– The National Economic Crime Centre

Examination of witnesses

Witnesses: Mike Haley, Dame Vera Baird and Wayne Stevens.

Chair: Welcome to this session of the Justice Committee and our inquiry on fraud and the justice system. Welcome to our witnesses, who I will ask to introduce themselves shortly. We first of all have to deal with declarations of interest by Members. I am a non-practising barrister and former consultant to a law firm. Any other takers?

Rob Butler: Prior to my election, I was a non-executive director of HMPPS and a member of the Sentencing Council, but I do not think it cuts across this.

Q1 **Chair:** I do not think there are any other relevant interests. Can we then come to our three witnesses and ask them to introduce themselves? Mr Haley, you are in the middle but virtual. Can you introduce yourself and your organisation?

Mike Haley: Good afternoon. I am Michael Haley, the chief executive officer of CIFAS, which is a not-for-profit fraud prevention organisation that has a membership of over 600 organisations sharing data, intelligence and learning, to prevent fraud.

Dame Vera Baird: I am Vera Baird, the Victims' Commissioner for England and Wales. In the last few months, we have done a report about typologies of fraud victims.

Wayne Stevens: Good afternoon, everyone. My name is Wayne Stevens. I am the national fraud lead for Victim Support, the largest independent provider of support services to victims of all crime, including fraud.

Q2 **Chair:** Thank you all very much. Dame Vera, your report talks of fraud having reached epidemic proportions. You certainly see it that seriously. We have seen fraud referrals to Victim Support, Mr Stevens, up by 59%, and some evidence that it seems to have got worse during the lockdown. Is that right?

Wayne Stevens: Yes, I am afraid so. It has been climbing year on year for four or five years.

Q3 **Chair:** That is what you have found as well, Dame Vera, I think.

Dame Vera Baird: Yes, that is right. It was not just during the lockdown and pandemic; it was growing anyway, but it has probably had an extra growth spurt.

Q4 **Chair:** What do you think caused that? Any idea? Have we had time to do any analysis as to whether there was an extra spurt or on what caused an extra spurt?

Wayne Stevens: Anecdotally, we can say that more people are shopping online. People have moved to online behaviours. The lockdown has contributed to that to some extent. We think there are also more young people using social media and online banking, so fraudsters have changed their modus operandi to make use of these emerging things. For instance, you may be aware of the WhatsApp fraud that is currently in circulation. It is a very new opportunistic thing. Of course, there are seasonal frauds like the HMRC frauds that come out towards the end of the tax year when people start receiving—

Q5 **Chair:** You get a bogus email, saying, "Do you accept a tax refund?", or whatever, and it is a non-existent account or one that scams your details.

Wayne Stevens: That's right.

Q6 **Chair:** I understand that. Mr Haley, do you have a view from your organisation's perspective about the main drivers of the increase both before the pandemic and then the extra spurt that Dame Vera referred to?

Mike Haley: We have seen fraud increasing for at least a decade. Before the pandemic, fraud was increasing as one of the most prevalent types of crime in the UK. We saw a levelling-off of fraud types during the pandemic—the fraud types that our members report—and that was linked to economic activity; 88% of the cases filed by our members through our system related to, or were enabled by, the internet, and the fact that many people were indoors and reliant on the internet, and many more people who were previously not internet-savvy or reliant on the internet had to be during the pandemic. A number of ruses were used under the cover of Covid—delivery scams in particular. Anyone expecting a delivery was getting phishing emails, emails that purported to come from DPD, Amazon and so on. People are expecting those click-on links and then their details are stolen for identity fraud.

Q7 **Chair:** Is there something that needs to be done by the internet providers in relation to that?

Dame Vera Baird: Yes, I am sure that they have a distinct role to play. How this stays, and whether it remains that fraud focuses largely—though obviously far from exclusively—online or not will depend a bit on how we carry on behaving after the pandemic or whether we resort to other things. Obviously, there is something of a decline in things like roof-mending fraud—"You've got some loose tiles"—because nobody was out and about.

As long as there is a lot of fraud online, there has to be some responsibility taken for prevention by those who have platforms that are made use of. I had both the HMRC one and the WhatsApp one, which was just an email that said, "I am your friend. Do you mind? I need to buy someone a Christmas present. They are very poorly. My bank somehow isn't replying. Will you buy me an Apple gift voucher for them?"

I knew this guy who was 90 and had no idea what an Apple gift voucher was. It did not succeed. The HMRC one was a quite scary phone call saying you have some major problem and you are going to be arrested if you do not contact this number straightaway. That is how people's guards are down: "It's my friend. I'd better help him." I am not thinking about me; I am thinking about that; and then, "Oh, my goodness, they're coming for me. I'd better shift quickly."

Q8 **Chair:** I had one from HMRC, and I had a constituent who was caught by the Apple one. It is very common. Does that fit with your experience too, Mr Stevens?

Wayne Stevens: Absolutely. There is a significant opportunity for social media and tech companies to get involved to prevent fraud. The online harms Bill making its way can be explicit about fraud, and there is also an opportunity to bring paid-for advertising into scope. We think that will make a significant difference.

Q9 **Chair:** Right, okay. That is not the case at the moment, is it?

Wayne Stevens: No, it is not.

Q10 **Chair:** That is very helpful. Do you think the public are aware that this is the crime they are most likely to be a victim of, or is it something they almost do not realise is there and that is why they walk into it so willingly?

Dame Vera Baird: According to CSEW stats and the work that my people in the office have done, it is 40% of all crime, which is an enormous amount, and it is by far the likeliest way of being victimised. I do not think that people are aware of how widespread it is.

There are campaigns of awareness often about specific things or specific types of fraud, and people perhaps take those in—things like messaging people. Mostly, if you do online banking, when you want to make a transfer they say, "Pause. Who is this? Have you transferred it before?", and so on. That seems to me a very effective thing to do. UK Finance has a system called "Take Five to Stop Fraud", which is the same kind of thing: pause and think, "Are you sure?" That kind of extra bit is a good warning.

A very important point is that you cannot leave consumers to protect themselves all the time and blame them if they do not. Yes, we need to raise awareness, but there is a finite limit to what individuals can do. It is also very clever, isn't it? You are easily trapped.

Q11 **Chair:** That is very true. It comes back to a point that Mr Haley might be able to start us off on. Are there particular interventions or resources that we ought to be taking to prevent people falling victim? The Association of Police and Crime Commissioners said to us that "we believe the best way to tackle fraud is to prevent victimisation." Do you get a sense that the victim feels that they are to blame because the bank says, "It was your fault," and so forth? Is there something we can do around that, or are there other things that we could do—either the internet providers or the providers of financial instruments that are sometimes the subject of the fraud?

Mike Haley: I certainly believe that this type of crime is not talked about because there is a certain blaming of victims or shaming of victims for being taken in by scams. First of all, we need empathy and messaging that will resonate, and we need to have individual contact with those who have been victims of fraud because often they become repeat victims.

What can be done about it? We were talking previously about the social media companies. Many of the scams are perpetrated on social media platforms such as Twitter and Instagram, and they do not have the messages. I will give an example. I talked yesterday with a campaigner about romance fraud, which is a type of scam where an individual takes advantage of someone's loneliness to try to develop a relationship. There were warnings on dating sites around Valentine's day, but not on the platforms the scammers have moved to. The messaging has to be timely and it has to be on platforms such as Instagram and Twitter where people are interacting with a scammer. Much more can be done by social media companies.

This year, they have joined an organisation called Stop Scams, which is a group of banks and other organisations, with the mobile phone companies and the tech companies, to start putting messages in the right place, but clearly they can do more. They are very good at writing algorithms to detect what I want to buy this year or what I am purchasing. I am sure their clever people can draw up algorithms to identify types of communications and advertising and take them down in a much more efficient way. We can stop this information, advertising and messages getting to the public on those sites.

Secondly, we should have timely messages. I do not think we have done enough research on what works. A lot of money is spent on public messaging by a variety of organisations, such as policing and charities. It would be really useful to understand, maybe from a psychological perspective, what messages work, in what format and in what language, to change people's behaviours.

Q12 **Chair:** Thanks. Are there any other observations? Mr Stevens?

Wayne Stevens: Last year, we supported almost 10,000 victims of fraud, and some of those people told us, "I didn't think that would happen to me." There is a widespread conception that fraud happens to someone else, that it happens to older people, vulnerable people or people who do not feel confident on the internet, but, in fact, it happens to any of us. There is a real role for banks to communicate honestly and directly with customers about the risk of fraud, about how to stay safe, about what to do if they become a victim of fraud, and, of course, where to get support, because it can be absolutely life changing. It can turn people's lives upside down.

Chair: Indeed. Thank you very much.

Q13 **Ms Abbott:** We were talking about types of online fraud. I heard on the radio last week about some poor woman who got messages from someone she thought was her son, and she ended up sending the person £11,000. Listening to her, she sounded so upset and almost like she was blaming herself for being taken in.

Dame Vera Baird: I think people do, very much.

Q14 **Ms Abbott:** Earlier in the month, the Prime Minister said that there had been a 14% drop in crime. In the end, the UK Statistics Authority wrote to him and said that it had actually been a 14% rise in crime and that he had not included fraud. Is there a case for not including fraud in the general crime figures?

Dame Vera Baird: No. I think it is excluded in some places for fairly obvious reasons. For instance, although it has not met for a very long time, I am on the national Criminal Justice Board case progression sub-group, which is about how to hasten cases through the Crown court. All of that work is done without fraud, because that would so distort it. If you have a fraud case at Southwark Crown court that takes two years to get to trial and another two years to hear and there are 4,000 victims, putting that into the system would distort it hugely, so it gets left out. I see that as completely rational, but I have always worried when attending something like that about how you focus on fraud if it is not in all of the mainstream activity about criminal justice and the system as a whole.

From my perspective as Victims' Commissioner, it is a serious problem giving people their victims code rights when there are 5,000 or 6,000 of them who have all been differently affected by some major scam. I do not think, in terms of the crime statistics, that there is any justification at all for leaving out fraud. It is really important given how big it is in particular, and that we are realising how impactful it is on a whole range of victims. There is nothing to be said at all in my view for not taking it very seriously indeed. It is under-reported, under-prioritised and under-investigated. Victims are under-supported. All of it is kind of second-rate crime; 2% of policing resources are allocated to it according to figures from the City of London police, who are the main force dealing with it, meaning that 2% of resources are devoted to 40% of crime.

Wayne Stevens: The Crime Survey for England and Wales estimated 5 million frauds last year and over 4 million victims, so it is very much a crime with victims at its heart, whether you have lost £40 on purchasing a pair of shoes online that never turns up, whether you have invested life-changing sums of money in what you thought was a pension scheme or a cryptocurrency, or whether you have been defrauded by someone you thought you were in an intimate relationship with. In some ways, it is a very personal and unique crime with significant, long-term emotional and psychological impacts for many.

Q15 **Ms Abbott:** That leads me to my next question, which I think we have touched on. What prevents individuals and organisations reporting that they have been a victim of fraud?

Dame Vera Baird: There are a number of barriers. Wayne, who is dealing day to day with victims, will be very well aware of others, I am sure. One we have touched on is the shame of it and feeling foolish. Older people sometimes lose a very great deal of money that they wanted to give to their children when they die, and it even ruptures family relationships because they are then ashamed and do not really want to see the people they intended to do well by and now cannot. You can see the emotional and traumatic barriers. Romance fraud must be particularly key. I do not think it is fanciful to associate it with the same sort of impact as rape or something like that because it is amazingly, intimately intrusive.

The other thing that is a problem is that there are innumerable organisations attached to dealing with fraud. Action Fraud is the receiving centre to which you are supposed to report, but only 5% of people asked by Citizens Advice in a survey last year knew what Action Fraud was. They did not report to Action Fraud because they had never heard of it. Most people will report to the police, who will probably send them to Action Fraud. Some of the stuff gets dealt with by Action Fraud, but quite a lot of it goes back to the police, so most people think they should go to the police.

The Serious Fraud Office investigates as well as prosecutes. Local standards departments do a lot of protective work and may be relevant to some. The CPS prosecutes fraud. The National Crime Agency looks at it when organised criminal gangs are involved. There is the National Economic Crime Centre. It is a sort of alphabet soup, and you have to work out to whom you should be complaining. There is a lack of clarity about how it is done. It goes to Action Fraud, it goes to the police, and it comes back to Action Fraud, perhaps. Who looks after a victim's interests along the way through that pipe?

Q16 **Ms Abbott:** Thank you. You have raised Action Fraud, and the Committee understands that Action Fraud is due to be replaced with a new reporting tool. What do you consider to be Action Fraud's main failings, and in what ways will its replacement need to be different in order to increase the number of crimes reported and then successfully investigated?

Dame Vera Baird: I think I understand what is happening with Action Fraud, which is that it is being recommissioned, and it might, in the best traditions of things that sometimes get criticised, be renamed. Probably they will call it Sellafield or something like that.

There is one particular advantage to the way it is going to be recommissioned. The City of London police, who had that responsibility, contracted to IBM, and IBM contracted to Action Fraud, whoever was delivering that. The commander of the City of London police did not have much direct input to Action Fraud, which was not a good thing.

I am glad that it is going to be brought into play again in that way. Clearly, it is the repository of first complaints, so it should have qualified first responders who know how to assess needs, vulnerability, repeat, all of that, and how to pass on to appropriate victims' resources if that is what is needed, which is pretty patchily achieved now. Then it needs to have plenty of information coming out, like the pathways and what will happen, and make sure that fraud victims, like everybody else, get all of their code rights as it goes along. It needs to be a proper, well-established victim support-type organisation, but with a specialism about fraud.

Ms Abbott: Mr Stevens, do you have anything to say about Action Fraud?

Wayne Stevens: I am better placed to answer your earlier question, which is about why people do not report. Embarrassment and shame because of the unique personal nature of the fraud often stops people. We worked with someone recently who had been telephoned by someone purporting to be from BT to sort out her internet, which was unstable, and over a six-hour call she was groomed and pressurised into parting with £18,000. She did not know who to tell and she did not tell her husband. Thankfully, she came to us.

Often it is being unaware of where to take it. Do I take it to my bank? Do I take it to the local police? Do I take to it Action Fraud if they are visible? Do I talk to the telephone companies? Do I go to trading standards if it is an in-person fraud? People often do not know where to go for help. The first-time response of those agencies is absolutely crucial for someone. If they ring their bank and the bank makes noises about the person not taking due care, they are unlikely to complain; they are unlikely to go to the financial ombudsman if they feel they have been treated unfairly, and, more worryingly, they are much less likely to report fraud if they become a repeat victim, and we know that many people do.

Chair: Okay, thanks. Mr Haley, anything from your perspective?

Mike Haley: I am part of the project that is looking to improve the Action Fraud and National Fraud Intelligence Bureau next generation product. There are two distinct elements. There is the national fraud reporting centre, which is the call centre. There is still a need for a central place for people to easily report fraud either online or on the phone. Mainly, that is because frauds do not happen in local police areas; they are dispersed. You can be a victim anywhere around the country. It is somewhere central. That intelligence is passed on to the National Fraud Intelligence Bureau, which puts together the packages of intelligence from multiple calls.

The issue is lack of capacity in the whole system end to end. You can produce intelligence packages, but they go to a local force that does not pick them up, and does not have the resources, competences and skills to investigate and also to interact with the victims. We need to look at the whole capacity of the system. Fraud is an under-resourced area, being 40% of crime and with only a small percentage of policing devoted to it. I think there will be improvements.

Whatever the centre is called, it will still be a reporting centre. Vera has it quite right. It was set up as a reporting centre, not as a victim service. There is a lack of empathy for victims and that core of education—how they can stop being a repeat victim—as well as taking the information around fraud. There is some hope that it can improve through the investment that is going in, but it will only improve from the victims' perspective if they see some outcomes and get some feedback. They report fraud and then they hear nothing much back. If you report a crime, you expect to be informed about what happens. That is what I would like to see.

Chair: Thank you.

Q17 **Angela Crawley:** Dame Vera, you mentioned the impacts, and much has been said about the emotional and psychological impacts. Could you perhaps outline clearly what you understand to be the main effects of fraud on both the individuals and the organisations that may have been targeted? Others may also wish to come in.

Dame Vera Baird: We may have touched on some of the impacts on individuals. Clearly, romance fraud is the one that has started to capture people's interest in fraud a little bit more. There is a sense of foolishness and of shame. It is quite misplaced because scams are amazingly lifelike, aren't they? With the more complex ones, you have a sense that the perpetrators worked on it for weeks and weeks and have an antidote or a combat technique to every psychological reaction to it that might allow you to throw it off or realise what it is, and they have worked out how to keep you in an iron trap all the time.

The shame is completely misguided, and then people feel they have let their family down. Older people feel that it is one step nearer their dotage and they are going to lose some respect from that. I imagine there is a whole gamut of emotional and psychological responses. Of course, people get ruined financially—not to forget that at all.

When we looked at the types of victims there are and came up with a great mixture of nine kinds of victim, which is a really broad categorisation, the impacts on each of them were quite different. I, a pretty simple soul, thought that if you gave them the money back, most people would probably be okay, but it does not work like that. We have a category of younger, high-harm victims who lose a little only, sometimes get it back, but seem to be really knocked back in their sense of social accomplishment. Perhaps as quite high-flying young people—I do not understand it in depth—they were impacted way beyond what I had expected, and way beyond what could be recovered by giving them back the money. All of this, it seems to me, needs to be looked at in considerable detail as we go forward, in appreciating what an impactful crime fraud really is.

Q18 **Angela Crawley:** You mentioned nine kinds of victim. Have you encountered specific demographics or particularly vulnerable groups who are primarily victims of fraud?

Dame Vera Baird: Fraud is very wide and there is a huge span of victimisation. Unlike lots of other kinds of crime, fraud is committed pretty anonymously, and offenders act without having a specific target in mind. Quite often there is less variation across demographics than you would see with other crime types. Interestingly, one of the findings in the research was, in fact, that adults aged over 65 are less likely to suffer fraud than younger groups, challenging the perception that this is a crime that specifically affects older people; but older people seemed likelier to fall prey to more serious and more impactful types of fraud, like investment schemes. Possibly people are thinking about what they can leave to their family and taking a last opportunity, as it were, to build it up. There does not seem to be a lot of variation of victimisation across the other age ranges.

There is a perception that fraud mostly affects the better off. People who are better off are searched for, but one of the groups, as I said, who are called medium vulnerability harm—younger, more urban, and more likely to experience harm—had the highest proportion of black and minority victims in this category, compared to other groups. There are nine categories that we found, and I can probably tell you about more as we go along if that is good, because I guess listing nine of them might not be too thrilling. It is very interesting indeed. Who needs help and who does not really need help will be something that we would like to focus on in a follow-up report, so that we can try to tailor some good support treatment from subsequent Action Fraud, or whatever it is.

Q19 **Angela Crawley:** That is very helpful. Thank you for those comments. We all have preconceptions of what a victim of fraud might look like, and it is helpful to outline that it is a very diverse group. Given that many victims of fraud report requiring no support, how can we ensure that the support is focused on those who need it most? Perhaps I will bring in Wayne, and then I am sure Mike will also have comments.

Wayne Stevens: Organisations that are being contacted by victims of fraud should be looking at impact rather than having preconceived notions of someone being vulnerable per se. We worked with someone recently who was retiring from the NHS. She was a nurse. She had received a pension pot. She was looking online for somewhere to invest that, and she saw an advert—a cloned website—for a well-known investment company. She clicked on the link, provided details and they contacted her, and she lost £26,000. She was absolutely devastated by what had happened. It changed the course of her life. The retirement that she thought she was going to have was no longer available.

She had a wide range of health impacts from that. She was sleepless. She lost her appetite. She was anxious and depressed. Thankfully, she came to us for support. We assisted her with recovering the money through the authorised push payment scheme. Her bank, thankfully, was a signatory. She does not fit into the normal typology of a vulnerable individual, and we find that quite regularly.

People can be impacted because of other circumstances in their life. They may have experienced bereavement or divorce, or they may have lost employment. That means that the impact of what has happened is much more significant. Those are the people we hope to reach out to—people who have been significantly impacted, irrespective of a vulnerability marker, or, in some cases, the size of the amount of money lost.

Q20 **Angela Crawley:** As you say, the impact can be profound and can be different for different individuals. Mike, do you have further comments that you want to make on those questions?

Mike Haley: I agree that we should concentrate our efforts on whichever definition of vulnerability we might come up with. For example, if you are poorer or elderly and not working, it is very much more difficult to recover from a financial loss. If you are working, you might put that down. You can say you will get it again.

One of the biggest issues is that we have a very patchy and inconsistent approach to supporting victims. The City of London police has a national victim care unit, which is good practice, but it does not cover everywhere, and not every police area has a victim care unit. We have a postcode lottery for what type of response you will get. There are some very good initiatives in some areas by police and crime commissioners—Hertfordshire and Surrey have good initiatives—but it is not widespread, and there is nothing to say that there should be national standards of victim care, and to see the best practice there is, share that and make sure that everybody who is a victim, wherever they live, has contact with someone who has empathy.

One thing I would throw in is that I visited the national fraud centre for Canada, where they employ people who have been victims of fraud. They are the ones who call up others who may have been victims, and they definitely can speak to them and have a connection, so that it is not someone just telling you from a law enforcement body who might not have the right impression of what it is to be a victim of fraud. My main point would be that there is complete inconsistency in how you are going to be treated as a victim of fraud.

Chair: That is helpful, thanks.

Q21 **Dr Mullan:** The feedback that I get from my local police is that an awful lot of the telephone and email-type fraud originates from outside the UK, so there are no realistic prospects of conviction in that regard. The treaties are not there, and, even if they were, given the amounts of money involved, while they are still hugely impactful to people, you are probably not going to extradite somebody for a £500 or £1,000 fraud. How do we marry up that we want to support victims, and that we want them to feel that we understand their distress and we care about what happens, with the fact that in many cases we may not be able to secure convictions?

Dame Vera Baird: I am sure you deal with this every day, don't you, Wayne?

Wayne Stevens: We do. Part of the solution is ensuring that victims are reimbursed. At the moment, the authorised push payment scheme is a voluntary code, and I understand there are steps to look at making it mandatory. We think victims should be reimbursed. That might not necessarily help them recover fully from the trauma. People often still take away feelings of loss of self-confidence and self-esteem, and fearfulness as a result.

Chair: Do you have anything to add, Dame Vera?

Dame Vera Baird: I am not sure that I have a great deal to add. Wayne is dealing with this through victim support units every day.

There is one thing, which is tangential, I suppose, but still a little bit to do with my various cohorts of people. How people are dealt with needs to be looked at more closely. There is what my research has called—a technical term—a middling group of people who number about a quarter, who do not really come to a great deal of harm at all and probably do not need an enormous amount of help. There is a cohort even broken down there of emotionally unaffected victims who have risky behaviours.

If you were able to categorise people thus, if these categories really work when you are talking about flesh and blood, you will be looking to that person about preventive measures and less risky behaviour, whereas the other severely harmed victims who are about 6%—the high vulnerability and harm cohort was in three of the groups—will need serious therapy or counselling of some kind. Dividing it up in that way can only be helpful and economic, really.

Dr Mullan: Mr Haley, do you want to add anything?

Mike Haley: First of all, I wonder if it is a bit of a myth that these fraudsters are overseas. Some are, but we do not know enough about it, and it can be seen as an excuse not to take action. Secondly, there are plenty of drugs that come in from overseas and we do not give up. We do not say, "That's coming from overseas." We use our diplomatic resources and our National Crime Agency resources to go after those who are perpetrating. We should use the same approach.

We have a diplomatic service. We have our National Crime Agency. The national economic crime command, part of the NCA, is starting to move in that direction. I definitely think we should not say there is anywhere that you can sit and feel comfortable about defrauding UK citizens. It is an issue of whether it is a priority for us. If 40% of crime is not a priority for us, it is never going to be a priority at this moment because it is the only crime that is going up. Let us use the resources we have to tackle at source—that is called upstreaming—as well as helping the victims and all the intermediaries who help launder the funds using British bank accounts, the money mules. I reject the fact that we should say, "It is probably overseas so let's not take action." We should have an organised strategy to deal with this.

Q22 **Dr Mullan:** Thank you. The Government are working on their fraud action plan. We have talked about the impact and the challenges, and you have touched on some recommendations, but what would be the things that you would like to see from the fraud action plan? We will start with you, Dame Vera.

Dame Vera Baird: It would be a great deal of public awareness and public education of a consistent kind, so that it is not coming from different quarters, and there is a recognisable place where you can be educated to take appropriate care of yourself and how you can be approached. Secondly, there would be somewhere you can check perhaps if something that you are starting to engage in is going to be a fraud or may be a fraud. Following from education, hopefully, more prevention might be in place, but it definitely has to be a higher priority for the police, who, as I say, spend 2% of their resources on what is 40% of crime, which is not very good. You have crime prevention officers in orthodox crime which is non-crime. You would hope for experienced people to be able to be around in a way that good old neighbourhood policing used to be, attending all kinds of places and warning about scams other citizens have come across, and trying to engage with people to protect themselves against all of that.

As well as prevention and protection, there has to be prosecution and not just an assumption that it is likely to be out of the country—Mike has just hit the nail on the head about that—and to pursue it properly. There is not very much fraud prosecution except the huge Southwark Crown court frauds that take up a whole place the whole of the time. You do not see, going around the Crown courts, as I do when it is practical, very much fraud that is there on the stocks.

Dr Mullan: Mr Stevens.

Wayne Stevens: As we touched on earlier, there is an opportunity for much greater collaboration between financial institutions, social media and tech companies, telecoms companies, law enforcement, and, of course, consumer groups to generate consistent, clear messaging around the risk of fraud, the impacts of fraud, what to do to report them and how to stay safe. There is also an opportunity for constituents such as yours to be passported to organisations that support victims even when it has happened. If there is little prospect of prosecution and enforcement, at least they may get some relief through being supported to cope, and recover from what is going on.

Lastly, there is probably some scope for improved international co-operation as well. We had a victim recently who was in a relationship with someone, and she passported money out to Turkey—£4,000 followed by another £4,000. On the third attempted transaction, her bank stopped it and said, "We think this is a fraud." She said, "What can I do?" They said, "You'll have to get in touch with the Turkish authorities to prosecute or to try to get your money back," so she was left. There is scope for international co-operation as well.

Dr Mullan: Mr Haley.

Mike Haley: In terms of what I think should be done? Is that what you would like to hear?

Dr Mullan: Yes.

Mike Haley: When we look at other types of organised crime, and much of the fraud is now being done by organised crime, we have what is called the four Ps approach: prepare, prevent, pursue and protect. There needs to be more pursuit activity. There needs to be a national strategy for fraud. We need more capacity in the system. The one thing that would really be a game-changer is to make fraud a priority under the strategic policing requirement. It is not a priority for policing because it is not in the SPR. That would make a huge difference to local policing activity.

Secondly, it is around the protection of people through good national messaging, co-ordinated across the public and private sectors. We can reach very many people from our members, for example, who can include all the banks, telcos and insurers. You can get messages in publications and communication through that, but we need to assess what works.

A national standard for victim care and what is expected from a victim nationally would then protect people. One thing you might be surprised to know is that there is no national strategy for fraud. There is an action plan, but it is a plan without a strategy. What are we trying to get to? What are our aims and objectives? What are the types of frauds that we think are most important to tackle as a community? In the private sector, we tend to suffer the costs. The individuals might get scammed or their identity stolen, but on the other side of that coin are institutions that lose money, and the cost of fraud is passed on to all of us in increased costs on our bills. Where is our national strategy for bringing everyone together?

Q23 **Dr Mullan:** In terms of specific legislation, you have mentioned the online harms Bill and you mentioned the code becoming mandatory. Are there legislative steps that you would like to see? I will begin with you, Mr Stevens.

Wayne Stevens: Apart from the mandatory nature of the code, the victims Bill is coming through as well, and it would be very effective to make fraud explicit in that, because it is a crime, and it is a crime with victims.

Dr Mullan: Dame Vera, either the victims Bill or the online harms Bill?

Dame Vera Baird: I guess we have focused less on fraud in the online harms Bill as we have been going along. We have just done an online survey, and we will see what comes out of that and whether it directs us in a particular way.

On the victims Bill, there was a very early thought that they had to review the new victims code almost as soon as it had been presented because the Serious Fraud Office was worried about how they could manage. In fact, they were inspected quite recently by CPSI, who inspect them too. I thought they were doing quite well keeping in touch with a great raft of thousands of victims. It was always done online, so they needed to have some back-up provision, which I was not so satisfied with, sound as the online stuff was, but they seem quite good, given that there are often very long delays in staying in touch and keeping people at least up to date with what is going on with the crime. They were also very adept at getting victims to give their evidence, because that is quite difficult.

As everyone said, a fraud executed in Farnham may have victims in all parts of the country, so you then have to think about getting people to court or getting them on Teams and so on in a sequence that lets the court work through. I thought that they were doing quite well with that. I am not saying it was really persuaded, but the MOJ went back on doing any kind of review. My basic view is that they are victims, and they are entitled to exactly the same as any other victim, and when there is no scope for a review, the pressure is on experts in the fraud area to do the job appropriately. I hope that does not emerge again. I guess there should be some kind of complaints system, which is a bit of a puzzle anyway, for the victims code, which is going to be statutory if it is broken. That is quite a hard thing to shape. We have had some attempt at doing it.

Currently, you just go straight through the complaint systems of each of the criminal justice agencies, but if what has happened is that you have not been kept up to date, you are not even at first base with the police complaints, with the CPS complaints, with the court complaints system or the probation service or anything, and you are likely to be further away, if you are in this flawed position where they are trying to keep in touch with 4,000. Conjuring some kind of way of ensuring victims code rights for such a mass of victims is probably a bit of a tongue twister.

Dr Mullan: Okay, thank you. Mr Haley.

Mike Haley: I echo my fellow witnesses on the online harms Bill encapsulating paid-for advertising. There is a danger of its just covering individual posts, and once those are criminalised it will divert activity to paid-for advertising. Bringing forward the economic crime Bill will strengthen Companies House, which can be used as a vehicle for setting up fraudulent companies.

For a number of years, we have been talking about or consulting on bringing in an offence of failure to prevent economic crime, similar to the failure to prevent bribery and corruption in the Bribery Act. The Bribery Act has been quite successful. Businesses are happy to implement those provisions. They could be quite easily expanded to economic crime, including fraud. Why do I think that will be a good thing? Instead of, as we are now, looking at various sectors that are starting to become vehicles for fraud, such as social media companies, it can move from sector to sector.

Other sectors of industry can be enablers of fraud but are not covered by any general duty to prevent economic crime, so they might not find that they are harmed themselves, but others are harmed. Therefore, bringing them in so that they have to look at how their services can facilitate fraud would drive a lot of activity by organisations to look at how they could prevent economic crime and have a due diligence defence, as you have in bribery and corruption. If they fail to prevent economic crime, they can face consequences.

Dr Mullan: Okay, thank you.

Q24 **Rob Butler:** I have a couple of follow-ups, if I may, to Dr Mullan's questions. On recompense, Mr Stevens, which you highlighted as the first aspect of how to help victims, do you think that should, to put it crudely, be a bottomless pit? How far do you think financial institutions and others should be responsible for providing money back to victims of crimes that they have not themselves been the cause of? I am very much playing devil's advocate here. If I have my television stolen, I cannot go back to the company that made the TV and say, "You have to give me a new TV." How far do you think that should go, especially as these crimes grow in complexity, and potentially in quantum?

Wayne Stevens: In terms of unauthorised fraud, if someone misuses your credit card, you will be reimbursed with no quibble, and that has been in place for quite a long time. With authorised fraud, where you have had some role in transferring money to a fraudster, it is unwitting and it is often done without people understanding the dangers and the risks of fraud.

As an industry and a system-wide issue, there is significant room for banks to improve what they do around transaction analytics. I gave the example earlier of the person who lost two lump sums and it was only on the third that her bank stepped in. There is a lot of scope to drive efficiencies within the financial system already, which will bring down the amount of money that is lost. Ensuring that banks are responsible for reimbursing people is one way of driving their efficiencies.

Q25 **Rob Butler:** Have you sensed any pushback from them on that? They could argue that it is not their responsibility; it is the responsibility of the person who presses the button and is misled.

Wayne Stevens: When someone presses the button, there is usually a genuinely held belief that what they are doing is a legitimate thing. I would want to go back to the step before then, which is to what extent the banks are telling someone whether that is legitimate or not. We have seen the introduction of confirmation of pay where you get some confirmation that the name that you think you are paying to is linked to an account. None the less, very little customer education goes on to help people to understand to what extent that legitimates who they are paying, and often it does not.

Q26 **Rob Butler:** Do you think that the fact that it is known that in many cases people will be recompensed to some extent allows the investigating authorities not to put so much emphasis on this because they think that actually perhaps less loss has been suffered compared with other crimes?

Wayne Stevens: I suspect not. Being defrauded is absolutely devastating. Even when people get their money back, they often live with long-term effects, so I do not think anyone acts with abandon, recklessness or carelessness when they are doing online transactions or when someone turns up at their front door and says, “Would you like me to repair your roof?”, because, of course, not all fraud takes place on the internet.

Q27 **Rob Butler:** But you have all suggested that fraud does not get the attention it warrants from the police and investigators. Do you think part of the reason for that could be that they think that the person has got the money back anyway? Could that be a factor? Feel completely free to say no, if not.

Dame Vera Baird: It would seem likely to me.

Rob Butler: It does?

Dame Vera Baird: I am not making the slightest criticism of the police. They have a lot to do. They can, and must, under the victims code, refer all victims to victims services where they should be able to get appropriate support. We have already discussed that it is not particularly good and there is not a lot of it, and it needs to be invested in. People who are very busy may well think that, if they have the money back and they are getting appropriate support for any emotional and psychological injury that they have suffered, maybe the priorities would go elsewhere.

Chair: A quick one from Ms Farris because we need to move on to the next panel.

Q28 **Laura Farris:** It will be a really quick one—just two technical questions. I have been reading about banking fraud. A typical retail bank fraud is where the fraudster uses the telephone number of the bank, which they have managed to copy, and then they get the person to transfer funds to a different account in that same bank. Obviously, retail banks have to know their customer obligations. It strikes me as extraordinary that they can just set up a bank account with Lloyds, Barclays or NatWest, get somebody to transfer money, and still there is not a mechanism for them to be repaid. You were talking a moment ago about whether the name matches. That is the only safety device that those banks rely on in order to repay. Do you think there is room in law for more stringent know-your-customer obligations on retail banks? That is my only question.

Wayne Stevens: I am not sure about the legal side of things, but certainly the fact that so much money gets transferred from one UK bank account to another—sometimes a mule account, sometimes a fraudster's account—suggests there is considerable room for improvement in verifying someone's identity when they first set up a bank account.

Dame Vera Baird: I suspect Mr Haley wants to answer.

Chair: Mr Haley, is there anything you would like to say?

Mike Haley: Thank you very much. It is a point well made. In fact, at the moment, the law prevents, or seemingly prevents, sharing about exiting customers for suspicion of money laundering with the next bank. Someone can be de-banked and exited from their banking relationship for suspicion of money laundering, and going to the next bank, opening an account and then using that account to send through funds. We need to look at the data-sharing laws and whether this is available through the Data Protection Act, which implemented GDPR, or whether there need to be specific provisions.

Effectively sharing data between financial institutions can close down some of the avenues for money to be exited from the system. If you can stop the money within the system, you have a better chance of reimbursing the individual, regardless of whether they have shared the blame under the code and whether they have authorised the payment. There definitely should be a look at that legislation. That should be allowable with the usual provisions around how we can share data in a proportionate and appropriate manner.

Chair: Thank you very much. I am sorry we have to move on to the next panel, but I am told that we are likely to have Divisions within the next hour, and that would interrupt us. Thank you very much to all three of our witnesses. I am very grateful to you for your time and your evidence. Many thanks.

Examination of witnesses

Witnesses: Commander Blackburn, Rob Jones and Mark Shelford.

Q29 **Chair:** Thank you very much for coming to give evidence to us, gentlemen. Perhaps I might ask you very briefly to introduce yourselves and your organisations, starting with Commander Blackburn.

Commander Blackburn: Good afternoon and thank you for inviting us. I am Clinton Blackburn, commander of the City of London police as national lead force for fraud on behalf of policing.

Mark Shelford: My name is Mark Shelford. I am the police and crime commissioner for Avon and Somerset and the national lead, shared with James Thomson, for economic crime for the Association of Police and Crime Commissioners.

Rob Jones: My name is Robert Jones, interim director general of the National Economic Crime Centre in the National Crime Agency.

Q30 **Chair:** Thank you very much. Mr Jones, how would you assess the scale of fraud at the moment?

Rob Jones: The scale of fraud is now well rehearsed; it represents up to 40% of reported crime and it is on the increase. More people have been forced online because of Covid. In relation to this threat the online world is very much a frontline for us. An awful lot of what is being perpetrated is in an online, non-regulated environment. It is now a volume threat that has grown significantly. The fraud figures, which are well rehearsed, of over 870,000 individual reports, create a real problem in the system in terms of volume and generating the operational response to tackle it, degrade it and push it back. There are a number of areas where we seek to do that.

Q31 **Chair:** Commander Blackburn or Mr Shelford, do you dissent from that, or can you add anything to it?

Commander Blackburn: I totally agree with what has just been said. We estimate that now it is at least 40% of all crime and it is on the rise. If there is no intervention, we reckon that by 2025 we will be looking potentially at another 25% growth in what is coming at us. When looking at law enforcement across policing, 1% of dedicated resource is funded to meet a threat that, as I say, is absolutely astronomical; it is huge.

Q32 **Chair:** We have referred to online as a trend. Are there any other trends being picked up, or is that the principal one?

Commander Blackburn: The top five that we have are online shopping fraud and auction fraud, fraud straight into cheque and plastic card, advance fee fraud, consumer non-investment fraud and computer software. They are the top five that we see. About 43% of victims are now being scammed online, and about 16% of all fraud that is reported has a link to social media platforms.

Q33 **Chair:** Mr Shelford, perhaps you can add to that, but also help me on what you think the state of enforcement against fraud is like.

Mark Shelford: I absolutely agree with what my two colleagues said as to the size of the problem. From an enforcement perspective, it is important that we do the prevention work and make the public as resilient and resistant as possible. We will come back to that aspect.

As far as enforcement is concerned, we also need to make sure that we have the right people trained as specialists and forensic accountants who understand banking systems; we need all of the cyber experts that conventional police forces generally do not have. We need to grow that capability as we face this growing threat.

Q34 **Chair:** Commander Blackburn or Mr Jones, do you have any observations on the enforcement side of things?

Rob Jones: It is recognised that the enforcement side needs to change significantly. We need it to move the dial for the experience of victims and contesting the space with the people behind these frauds. The observation about specialism is well made, but if you make it specialist, you risk making it hard to do. There is something very straightforward about what is playing out now in the digital age, and mainstreaming that into policing and the response is a big part of what we need to do.

Yes, there are complex frauds that need highly complex investigative and prosecutorial responses, but a lot of it is relatively simple and is perpetrated online. Engineering that out with social media companies and exploiting the ability to prevent it, because it is playing out online in plain sight, while going after the complex end, is what we need to do, but we need to make it mainstream. The digital investigative response in identifying and investigating the threat online and dealing with the disclosure tail behind it all has to be mainstreamed to deal with the volumes we are talking about. There are more complex issues, which we will come on to, at the high end, but the volume response needs to be an integral part of policing.

Q35 **Chair:** Commander Blackburn?

Commander Blackburn: I would not fall out with anything that has been said. A few fundamental things have to change. Fraud has to be recognised as a priority. We are starting to see some of that play out in the online harms Bill, which will be a significant step. Having it in the strategic policing requirement would also be a help.

One of the things we are doing as lead force is to start to work really hard with all of the 43 forces across the country, because we recognise that they all have their own significant challenges. There are many priorities and different threats, and they have a finite number of resources to meet them. As a result, chief constables have some difficult and challenging decisions.

That said, fundamentally, the system and how we are set up to navigate it and respond to it is right, with NECC as the system leader and everything else we are trying to do with the various agencies that take on fraud, but without the right funding and resourcing to meet this massive threat it will be forever challenging. Chief constables having force performance boards and PCCs' crime plans—all these subtle things—will go to make a sea change across the whole system.

Q36 **Rob Butler:** Are there any specific difficulties you face in identifying frauds and then conducting successful investigations into what you have identified?

Commander Blackburn: Not necessarily in identifying them. There are 56 different fraud types. They climb all the time as they find different avenues and new ideas. In the Action Fraud system and the reporting system, sometimes victims struggle to identify what has happened to them because perhaps they do not recognise the offence types. In capturing the offence type, I do not think there are any issues with the actual recording of it, but there are various responses. Given 56 types, there are lots of different vulnerabilities with different types of crime. Which one is more important than another? There is only a finite number we can investigate.

Q37 **Rob Butler:** Mr Jones, you said that you thought a lot of this fraud could be considered at a fairly general level. Does that mean, therefore, that the skills of the officers can be fairly general and you are not looking at ultra-specialist officers for the vast majority of the frauds?

Rob Jones: This is a mixed economy, but you need digital natives and people who understand online. When you are dealing with someone who has been the victim of an online scam and starting a proactive investigation into it, unless you have the basic skills to understand that and do it, you will not progress quickly.

Coming back from that to before the offending happens, or preventing the offending from happening, there is so much opportunity in the space of payments for the banking industry working with law enforcement, and for victims, fully to understand how fast the payments work, confirmation of payee and what it may mean if you are transferring funds and you cannot do that. Therefore, you pivot back. If you create resilience in victims, you need a local response that can speak digital and is digitally savvy. If you are going to investigate a crime that has happened, you will need basic skills in digital forensics in the online world, and if you are to prevent it you need to understand the online world and operate in it, as we do with child abuse and other threats, to push into that space and contest it.

Q38 **Rob Butler:** Given how much in demand cyber experts are, how straightforward, or not, is it to recruit and retain the sorts of people you need to do what you have just described, particularly when you have a private sector that is also very keen on those people and has a huge amount more money to pay them?

Rob Jones: There are a couple of things, and I am sure that Clinton will speak about this as well. When we talk about cyber expertise, we cannot excuse the fact that digital is now mainstream. My point is that there is high-end cyber expertise that can reverse-engineer malware and can operate online covertly, but that is not really what we are talking about with so much of this. It is more about a basic understanding of the digital environment and being able to operate in it and mitigate the threat, risk and harm that is there.

We have that expertise. It is hard to hold on to. Once people are trained, they become a commodity and they will get life-changing offers to move away from law enforcement. We need an attractive offer on professional development; we need internships and apprenticeships—all of the things we are doing in the NCA—to drive up that expertise. Meanwhile, in the police uplift programme and elsewhere, you need that at scale.

Rob Butler: Commander?

Commander Blackburn: I agree. We see significant losses across the policing landscape in terms of training people up at significant cost to the public sector. They move to the private sector for much higher recognition financially.

I want to touch on the fact that as national lead force we are also the single provider for training across policing for fraud, outside the College of Policing. One of the things we will be doing under the next generation of the Action Fraud system is launching an app for all frontline staff, which will, hopefully, come out in August 2022, so that frontline staff who are at the scene of a fraud or cyber-crime will be able to get advice quite quickly on best practice for the victim and best practice in securing evidence. There is a lot to be done on that.

I think we trained about 1,000 staff last year across fraud, but fundamentally we need to look at how police officers going through their probationary period are trained. If you are talking about 40% of all crime, it is only going up. To some extent, we are probably putting a huge amount of effort sometimes in investigating the old crime types, like burglary offences, when offending is moving on and perhaps the training programmes being delivered to police and other law enforcement have not caught up at quite the same pace.

Q39 **Rob Butler:** The armed forces are being more flexible in the sorts of people they recruit to deal with cyber-attacks against national critical infrastructure, for example. Are you doing the same in police recruitment by, for example, not necessarily requiring people to do exactly the same fitness tests or have exactly the same aptitudes? We know that quite often people who are brilliant at digital may not tick the boxes that are required at other points, if I can put it in that fairly crude way.

Commander Blackburn: Policing moves quite slowly. I am just coming up to 30 years in policing. I do not think that fundamentally training has changed massively. The introduction of public protection-type training has become much more on the radar, but not a huge amount else has really changed.

I think we have moved on with things like the Police Now scheme where you can join as a direct entry detective and go into different areas of policing without having gone through the traditional two-year route of frontline response officer. It is absolutely on the radar in the conversation being had about how we can get professional people to come in from a cyber background. You might now have police as cyber investigators, for example, as opposed to just detectives, but we are not quite there yet. It is very early stages, even at a conversation level at the moment.

Q40 **Rob Butler:** Mr Jones, do you want to say anything on that?

Rob Jones: I recognise the challenge in relation to that. We have a different route into the NCA for our programme and how we bring people in, but there are similar challenges. It is probably easier for us to bring in a different type of candidate.

Q41 **Rob Butler:** Mr Shelford?

Mark Shelford: The secret is being as creative as we can, as well as having a structural solution. In Avon and Somerset we have a very good relationship with the University of the West of England. The faculty that deals with training new police officers is next door to their cyber faculty, so there is a lot of cross-work, as well as around the use of volunteers and, if you like, special specials in this field. We have to acknowledge that we need more. We need those specialists, but we also have to try to train our mainstream officers in these fields. That work is starting, but I would not say it is anywhere near where we want it to be.

Rob Butler: Thank you.

Q42 **Dr Mullan:** I want to pick up on the effectiveness of enforcement. Of this high-volume crime, as a percentage how often are you able to identify a perpetrator at the moment?

Commander Blackburn: We are not able to, given the different systems across the police—for example, the arrest rates or the volumes. What I can say to you, as Rob has already said, is that of the 875,000 reports that have come in, 58,000 were disseminated across policing in 2021. There was an outcome rate for that year of 4.5% in actual judicial outcomes.

Q43 **Dr Mullan:** So roughly 800,000 were not even sent out to forces; were they discounted as non-pursuable, or what?

Commander Blackburn: Not necessarily non-pursuable. They go through various streams of threat, harm and risk assessments—or THRIVE, if you like. They look for viable lines of inquiry, for vulnerability and certain levels of loss. There are lots of different factors in each of those different crime types as to what will ensure it goes out to a force as a dissemination because it is felt that there are viable lines of inquiry.

Q44 **Dr Mullan:** We probably hear from constituents who may have lost a few thousand pounds and have a funny feeling that they do not get past the first filter, and nothing happens, essentially, from their point of view. Do you recognise that picture?

Commander Blackburn: Yes. I am fully aware of MPs' postbags filling up with complaints being sent through. It is really challenging. Every report gets some level of service, whether it becomes intelligence in the system or whether it is protected via victim contact, because we have the economic crime victim care unit as well. Anybody's case that does not get a service will always get contact from our national economic crime victim care. Unfortunately, not every single case can be investigated, just because of the sheer volume. Even when you look at what we are sending out to policing, there are then 43 different THRIVE processes, exceptions and priorities. It may be that, even though we disseminate it to a force, that force does not investigate it because it does not hit their priorities.

Q45 **Dr Mullan:** In the same way that they might not investigate shoplifting.

Commander Blackburn: Yes.

Q46 **Dr Mullan:** We were talking earlier about where perpetrators are located. Do you have any insight as to whether a lot of it is coming from abroad?

Commander Blackburn: How scientific this is, I cannot guarantee, but we have just done some work with the National Fraud Intelligence Bureau looking at 2020 and 2021 and the entirety of the offences that came in. What we are able to say from that, crudely, is that 30% of those were completely international and 47% had a UK and international tie. If we tie the two together, about 77% had an international bit and 23% were solely from within the UK.

Chair: Thanks very much.

Q47 **Ms Abbott:** Commander Blackburn, to what extent is fraud a real priority for the City of London police, and what sort of fraud is a real priority for your force?

Commander Blackburn: That is a good question. Fraud is an absolute priority. It is one of our top priorities in our force and is in our crime and policing plan, and we are obviously trying to make it a priority for every other force, which is why we are really busy doing the engagement work. We are visiting all police forces this year. In terms of the ones I talked about, the annual assessment identifies the top eight areas of criminality and five of those I listed not so long ago were in online shopping, auction fraud and so on.

Q48 **Ms Abbott:** We are taking evidence from three different organisations. What can be done to increase collaboration across bodies working in the fraud sphere to increase the sharing of intelligence and improve investigations?

Rob Jones: I can give you the National Economic Crime Centre perspective. It is central to the mission for the centre. It was set up three years ago to drive and improve it and it is doing that. It is a multidisciplinary environment with all of the agencies involved in the fraud response within it. With City of London, we have been tasked under the Crime and Courts Act with driving the national response, using the legislation that we have.

What we have done is simplify the governance, where we can, and thin it out and make us able as a team to work across national policing and get work out of the door to forces as quickly as possible to improve the pursue response. Everything we now do is about moving the dial in our operational effect, but establishing that platform has been challenging. We have now established it and it is working and we are starting to see the results coming through in what we do, but we need to accelerate it to start to degrade the threat.

Q49 **Ms Abbott:** Why was it challenging?

Rob Jones: Because, as you alluded to, when we started this journey there were multiple different organisations that were disconnected, had different priorities and different strategies, and were working on different niches of the threat. There are a number of enablers that are consistent across fraud and economic crime. Bringing all of those individuals together into the same environment has been incredibly powerful and positive in achieving common objectives and moving forward to a point where we have an effective national fraud strategy and we can develop that, with partners, to move it on.

Q50 **Ms Abbott:** Mr Shelford, as a PCC do you have any thoughts on better co-ordination?

Mark Shelford: Absolutely. It is vital that we have better co-ordination. For example, I and James Thomson wrote to all the PCCs in January encouraging them to make fraud a priority, particularly around the teaching, education and resilience of the population. That has been very well received. You will be pleased to know that all of the police and crime plans reflect that. That is one successful aspect.

For a lot of county police forces the issue is understanding co-ordination between what is local and regional and what is national and international, and the part that they and all the different agencies nationally with a foot in this have to play. If you look at your Twitter feed, you will see many different people giving you advice on how to deal with fraud. They quite often say the same thing, and making sure that we co-ordinate all of that activity across the spectrum is very important.

Q51 **Ms Abbott:** Commander Blackburn, the City of London must have established relationships with the private sector. How do you currently work with the private sector to gather intelligence and identify potential risks of fraud?

Commander Blackburn: We have had some strong relationships over the years. For example, there is a joint team with the Metropolitan police, the City of London and UK Finance. With the ABI and the insurance industry, we have another team looking nationally at insurance fraud. On intellectual property, we have a separate team, and we also work with the movie industry. We have seen some successes through even just those three teams by combining that extra resource with industry.

Another example would be through one of the major banks under project OLAF, which for the first time ever in the UK was unleashing frozen funds. That has now seen the roll-out of a national economic crime unit to all the other police forces in the country that did not have it. It has also provided a cyber team to take on more crimes coming into the DCPCU unit in terms of UK Finance. We share intelligence with industry, with NECC as the system leader.

I want to touch on this briefly, picking up what my colleague said. I feel that, a couple of years down the road, NECC is starting to find its feet, drive activity and corral all the other organisations that form part of it. It is through the NECC that those sorts of strong relationships are beginning to be built with telcos and other organisations. There is still a lot of work to do, but we all feel that it is moving in the right direction, although perhaps not fast enough to meet the demand and the outcomes.

Q52 **Ms Abbott:** Could you improve the use of intelligence?

Rob Jones: We can always improve the use of intelligence. In relation to fraud specifically, our focus has to be on dealing with it as a crime in action, not dealing with the consequences of the fraud and trying to investigate it after it has happened. That means using intrusive covert intelligence tactics against targets that we believe are involved in fraud, to act much more quickly before the money has been transferred and before the fraud has been perpetrated and the victim has been victimised. That is a shift in the investigative mindset that we are pushing hard, and a cultural challenge in the way that people have traditionally investigated fraud.

There is a big focus on dealing with the data from crimes that have been committed, joining the dots and improving understanding, but our focus from an NCA perspective is to push hard to deal with these things as crime in action and prevent money being transferred, through offensives against money-laundering tsars, intervention through the fast payment system, or whatever we can do to prevent victimisation and identify the suspect and make an early intervention with a different type of arrest from what we have traditionally seen in fraud, because we will not get through the volume—we have all heard what it is—if we are acting after the event in all these cases.

Commander Blackburn: With the next generation system of Action Fraud, we have something called Project Recall, which identifies money at risk and alerts the bank, so that it can prevent it from moving on or try to recover it. One of the facilities the next generation system will have is to automate that and make it a lot speedier, so it is about sharing intelligence quickly with those other agencies.

Q53 **Ms Abbott:** Mr Shelford, do you know what the process is for regional forces investigating crime when the perpetrator is based outside their geographical boundaries?

Mark Shelford: I think that is an operational question that would be better going to Commander Blackburn. My understanding is that it is passed down from the City of London Police via the national bureau and a decision is then made as to whether it goes to a regional force, the ROCUs, or a county police force for investigation. For technical, you need to go back to Commander Blackburn.

Chair: Commander Blackburn.

Commander Blackburn: That is correct. Everything is reported to Action Fraud and will go through their processes. They will identify where something that has viable lines of inquiry can best be investigated, and then it will be allocated to that force. If you end up at the next level up and it is starting to cross many borders, it will go to a regional ROCU which will then investigate it. If it starts to cross multiple counties, and potentially countries, it will come to the national lead force, which is us, City of London, which takes on the really big cases that fall under the threshold of going into the NCA.

Chair: Thank you very much.

Q54 **Paul Maynard:** If I get cut off, I apologise. Everybody here is saying that we have to tackle fraud and it is really important, yet arrayed before us today are one interim director general, one temporary commander and one shared lead. I do not know how often PCCs play musical chairs with their lead roles. Is it every four years? I don't know. With this lack of continuity, I struggle to believe that there is any focus among the law and order communities to deliver on the idea of tackling fraud. Are we being unfair on you all? Do your talents far exceed your temporary job titles?

Rob Jones: I have 35 years of law enforcement experience and I have been responsible for tackling all of the SOC threats, with a range of different tactics.

The reason I am an interim director general is that our director general moved on at short notice because of a health issue. We have an interim director general, Graeme Biggar, who is the substantive director general. I stepped up to that role to deal with the National Economic Crime Centre and the rest of the SOC threat, as I have been doing for many years. This is not something to do with continuity and focus. We have a laser-like focus on fraud and economic crime. We host the National Economic Crime Centre. I would not want you to think that, because there is "interim" in front of my job title, the NCA is not focused on fraud.

Q55 **Paul Maynard:** I am sure you all are. It just suggests a certain fluidity in the approach, with all these different alphabet soup arrangements. Commander Blackburn, tell me I am wrong.

Commander Blackburn: You are wrong. I can see where you are coming from. Certainly, in policing we move around different areas of responsibility and there are lots of different crime types. That is why it is so important that the national lead force has the specialism within that command. For example, the post I came out of a year and a half ago was as detective chief superintendent overseeing national lead force operations, so I come from that background. Likewise, the assistant commissioner who has just taken over the post occupied pretty much every single rank after sergeant in that command.

We have many staff who have dedicated their whole careers to sit in that command. The positive thing is that, if I was to step out tomorrow, it would make no difference to business as usual in driving activity, because we are leading against national plans and economic crime plans. We are all part of the NECC and know exactly which way we are driving.

Q56 **Paul Maynard:** There are loads of fingers and loads of pies; it is alphabet soup. It is still quite hard to get to the bottom of it. Do you want to tackle fraud? Everybody says they want to tackle fraud. There are 5 million a year and seven committed every minute.

What I am not clear about, having sat here since half-past two, is what having tackled fraud would look like. How would we know that we have tackled fraud? Would it be that every single one of the seven a minute had a Rolls-Royce service? We cannot achieve that even for domestic burglary. That concerns my constituents. What would a reasonable expectation for tackling fraud look like? Maybe Mr Shelford as an accountable PCC might have a view on that. What would be realistic to offer those who live in your area?

Mark Shelford: It is very important that we look at this both before the event and, if the event has happened, after the event. Before the event, we need to focus on making sure that the population is educated to be more resilient and resistant to this type of crime. In Avon and Somerset I am in the process of sending out a postcard to all over-60s—what we used to call in the military a FLAP sheet. If they feel that they are under any type of fraudulent attempt they can deal with it; they can go through that postcard.

If there is an event, the county police force needs to be able to deal with it. We need to be able to investigate and prosecute it. We need to make it a hostile place for criminals who wish to commit any type of fraud, but we also have a responsibility to victims. The fraud protection officers and vulnerable victim fraud officers we employ in Avon and Somerset go to look after those victims to help them in any future prosecution, and to make sure that they do not fall for the same sort of thing again, and to stop revictimisation. That has been a terrific success. In quarter 1 this year, our revictimisation has fallen by 9%.

You need to look at the continuum from start to finish as a complete package. I come back to the most important thing in all of this, which is educating the population and making sure that they are as resilient and resistant to this type of crime as we can make them.

Q57 **Paul Maynard:** I almost took the message from that that you feel you have tackled fraud already. I am sure that is not quite what you meant. Do you think that the £400 million allocated in the spending review is enough to tackle fraud?

Mark Shelford: There is never enough; we need more absolutely, but we need to work with the tools and resources we have at the moment to maximise their effectiveness. I do not want to play buzzword bingo, but it is so important to be imaginative and creative in the way we do this. I talked earlier about using volunteers and connecting with universities, where you have that level of expertise, focusing on the really important pieces around cyber and generating the expertise in your force to deal with it.

Q58 **Paul Maynard:** Mr Jones, will the £400 million be enough to get you to the position where you can say you have met your own definition of having tackled fraud?

Rob Jones: It will make a significant difference. That dedicated resource and the three-year SR will make a big difference to planning and moving the dial and is really helpful.

You ask a really good question about the end state and the theory of change. Where does this go? We have an unregulated environment that is used to perpetrate fraud against a regulated environment, so the financial sector has been on a very different journey from the west coast social media companies and the internet. We have a massive disconnect in the way that works. The people who perpetrate these frauds operate in a free-wheeling international environment that is completely unregulated. That is how they victimise people.

Things like the online harms Bill and our ability to tackle people online will prevent abuse of the regulated sector. Working with the regulated sector, with UK Finance and others, we will be able to inform victims, create resilience and prevent payments from being made. If you focus on payments, many people will not be victimised. A little bit of friction in the system around faster payments, which made people think twice about who they were sending money to, could make a massive difference.

Moving this on, so that the payments are not being made, is a significant thing for all of us. Being able to bring people to justice so that they are not emboldened and victims see a result is important, but preventing it from happening in the first place is really important—Mark's point—because so much of it is preventable. It is a familiar story for all the online crimes. With child sexual exploitation and cyber-crime, the internet-enabled age has created the ability to victimise somebody remotely, and that is what we need to focus on.

Q59 **Paul Maynard:** Commander Blackburn, we have heard today from Sir Michael Barber with a sneak preview of his policing report. He has done a webinar talking about how the national police computer is now 50 years old—older than I am. I can scarce believe it. He talks about a Betamax police force chasing blockchain criminals, suggesting that you are all antiquated and out of date. Do you recognise that description of you in your anti-fraud role because, surely, you are facing the most technologically sophisticated criminals there are?

Commander Blackburn: Some of the systems could probably be classed as antiquated, but again it comes down to investment.

Q60 **Paul Maynard:** Is the £400 million enough?

Commander Blackburn: The £400 million will give us a good head start in turning some of the tide. *[Interruption.]*

Rob Butler: You have been saved by the bell.

Chair: You think that £400 million is a start.

Commander Blackburn: I think it will give us a really good start in making change. With the protect network that Mr Shelford talked about, it is important to get the messaging right at the front end before people even become victims. I do not believe we will see the money for that protect network coming through until year three. It is a shame we could not get it in year one.

Q61 **Chair:** I understand that. There is one final question I want to ask before wrapping up, because we have a number of votes and you would be hanging around for ages. Are you involved in the development of the Government's upcoming fraud action plan?

Commander Blackburn: Yes.

Rob Jones: Yes.

Q62 **Chair:** All of you are. Are there any particular things that should be in it?

Rob Jones: Everything we have been discussing: public-private partnerships; payments; digital; and the criminal justice system in terms of disclosure and how we operate digitally. Those big topics are the things we need to address as part of it.

Chair: Everybody appears to be nodding in agreement with that. If there is anything else, drop us a note. That will be the easiest way to deal with it. If there is anything else that you think we should put in our report, or that the Government should add, perhaps you could let us know.

I am sorry it is a bit truncated, but we have got through the bulk of your evidence. We do not want you hanging around because we just do not know how long this vote will take. Thank you very much for your time and evidence. The session is concluded.