HOUSE OF COMMONS

Treasury Committee

Oral evidence: Economic Crime, HC 940

Tuesday 8 January 2019

Ordered by the House of Commons to be published on 8 January 2019.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Steve Baker; Colin Clark; Mr Simon Clarke; Charlie Elphicke; Stewart Hosie; Alison McGovern; Catherine McKinnell; Wes Streeting.

Questions 564 - 622

Witnesses

I: Police Commander Karen Baxter, Police National Coordinator for Economic Crime, City of London Police; Detective Chief Superintendent Peter O'Doherty, Head, Economic Crime Directorate, City of London Police.

Written evidence from witnesses:

– City of London Police

Examination of witnesses

Witnesses: Karen Baxter and Peter O'Doherty.

Q564 **Chair:** Good morning and thank you very much for being here for this first Treasury Select Committee meeting of 2019 and our next session on economic crime. I am going to ask both witnesses to introduce themselves. Detective Chief Superintendent, we have had a debate about how to pronounce your surname, so you will have to help us on this. Commander Baxter, perhaps we can start with you. Could you just introduce yourself for those watching?

Karen Baxter: I am Karen Baxter. I am the Commander for Economic Crime for the City of London and the national coordinator.

Peter O'Doherty: Good morning. I am Detective Chief Superintendent Pete O'Doherty, and I am the directorate head for the Economic Crime Directorate for City of London Police.

Q565 **Chair:** Thank you both very much indeed for being here this morning. We are very grateful to you for your time. Perhaps I can get straight into the questions. The City of London Police, in evidence to us, said that they had requested partner bodies to close 170,000 bank accounts, websites and phone numbers linked to fraud, but UK Finance figures showed that just over £500 million was stolen through authorised and unauthorised fraud in the first six months of 2018. This sounds like a bit of a war on consumers and against financial institutions. Are the authorities winning the war, or are the criminals winning the war at the moment?

Karen Baxter: The first thing is that, for the first time in probably about five or six years, we are looking at having a very joined-up, co-ordinated approach across all of law enforcement. This is something that extends way beyond policing. The introduction of the National Economic Crime Centre recently in October 2018 is a really good step that brings all of the assets across law enforcement together and extends that further into partnership with finance and with banking. That has a tremendous opportunity going forward around addressing all of the issues in economic crime.

If you put in context where we are in 2019 and where we were in 2013, when we introduced Action Fraud, we have a very different operating environment. In the interim, we have reduced headcount and we have reduced finances, but we have a very different operating context, where we have an increase in counterterrorism. What that means is that, in some respects, fraud and economic crime has been less of a priority for policing. When we look at the National Economic Crime Centre and the establishment of that model across all of law enforcement, there is a renewed focus. Certainly, when I came into post in July of last year, what I found was a real willingness across all law enforcement to work

together to exploit the assets that we have and to really start to address this.

We are not where we would wish to be but this is a really good first step around taking it to the next phase. Part of that will be about understanding not just the data that we have but how we use that to deploy the assets that we have across all of law enforcement, and also into the private sector and how we inform the public.

In terms of the issue of how we win the war against economic crime, I am not sure that those are terms that I sit comfortably with. What we do is we use all of the assets, publicly and privately, and use those to address criminality. We are in a good place. We need to be in a better place but there is a collective will that we will take that further forward.

Q566 **Chair:** Detective Chief Superintendent, do you have anything to add?

Peter O'Doherty: Yes. In terms of the specific question around the identification and disruption of these enablers, like websites and bank accounts, the UK is in a very strong position. If I can give two quick examples, a significant part of our investigations that get reported to Action Fraud have a cyber-enabler—for example, a website. Where that website is a .co.uk domain, we work with Nominet, which, normally within two days, disrupts that platform. If you compare that to the United States or a European counterpart, they invariably have to go through a court process to get a production order.

Secondly, there is the relationship with the UK banking sector around the disruption of bank accounts in real time that prevents victims losing thousands and thousands of pounds. This relies upon a very close relationship with banking. In fact, unlike most countries I have come across, we receive intelligence from the UK banking sector to add value to the crimes that we get through Action Fraud. Again, that relationship is very unique to UK policing and is one that I have not witnessed commonly across the globe.

Q567 **Chair:** We are going to explore some of the points that you have made. That close relationship between private and public is a very valid point. We have done evidence sessions on what I would call major economic crime such as terrorist financing and money laundering, but much closer to home and closer to our constituents will be the issue of authorised push-payment fraud, where life-changing amounts can be taken from people's bank accounts with absolutely devastating consequences. Of course, sometimes it can even drive victims to suicide, for example. The figures show that only £1 in every £5 of an authorised push-payment fraud is returned to the victim. Why is that the case, in your opinion, DCS O'Doherty?

Peter O'Doherty: There are a number of reasons. In some cases, victims—and particularly the banking sector—do not report crimes to Action Fraud, for example, so that limits our understanding around

impact and the trend and typology and, therefore, inhibits our ability to provide an evidence-based policing response. Secondly, some of the monies that are taken from victims are laundered outside the UK jurisdiction. Once that money leaves UK shores and is laundered through different payment devices and platforms, it is really hard to get the money back.

The UK Government have recently updated legislation under POCA—the Proceeds of Crime Act—and policing has more tools than ever before to deny those assets and get money back to victims, but it is invariably an arduous process that can take a long time. It is the whole issue around the war, and the sheer volume of what we are facing makes it very difficult. Then you go into discussions around digital currencies, like Bitcoin and Ethereum, where policing's knowledge of how those payment platforms work is limited and growing each day.

What I would say is that the banking sector is working proactively to build security by design, so increasingly working with policing to understand how these crimes happen and how to prevent them at the initial gateway.

Q568 **Chair:** Just before I hand over to Charlie, you mentioned the improvements made in the banking system. One of the things that colleagues might come on to but which I noticed in our packs was the introduction of chip technology on cars and how the UK has led the way in that. Would you agree that one of the other vulnerabilities is that, if fraudsters are finding it harder to access bank accounts, they are going to the consumers themselves. Is there much more that needs to be done around educating consumers and making people much more sceptical about messages and communications that they receive and handing over details? Where do you think the UK is in that part of the battle, Commander Baxter?

Karen Baxter: We are in a pretty good position. We have a really strong protect network. We work with the private sector and with all of our law enforcement colleagues around trying to get that information out to the public. You are right that we have to constantly evolve because what happens is that criminals will do something and we respond to it. When we respond, they change, so it is a constant and very quick turnover in that evolution cycle, as I would call it.

We have quite strong protect networks. We are very active in terms of our social media. In terms of dealing with victims, we are looking at how we more quickly engage with victims and give them some bespoke assistance. Some victims will appreciate a call or signposting; other victims will need more of that. Every call to Action Fraud is, on average, 19 minutes. What we do on top of that is that we follow up with some of those victims. We have been—very gratefully—funded by the Home Office around developing a victim care model that helps us do that.

It is about stopping victims in the first place. It is about protecting them, because what we know is that some victims will then be susceptible to reoffending. That is the benefit of having a lead force and about having Action Fraud, because we can identify that pool of victims who might then be susceptible to reoffending, perhaps in six or eight months.

We are doing a lot. Again, we will continue to do more. The issue for us going forward is about really understanding the analytics of the emerging trends, getting upstream of those and making sure that we educate people. That is one of the benefits of having a police service deliver this, in that, if you look at the diversity, the volume and the complexity of fraud, you have very different messages for very different sectors. What we would provide as a message to, perhaps, an older person living on their own in a rural location is somewhat different to what we would advise in terms of banking. What we have is the capacity. Through 43 forces, through the ROCUs, through the City of London and our connections with the banks and law enforcement, we have the means to bespoke and adapt that messaging to the people who need to get it, when they need to get it.

Q569 **Charlie Elphicke:** Good morning. Commander, just looking at what UK Finance has been saying, it seems that crooks have stolen £500 million through fraud scams in the first half of 2018, so this is a £1 billion a year problem. What types of consumer economic crime do you see being reported the most?

Karen Baxter: If I can refer to my notes so that I am accurate on this, in terms of the types of economic crime that we have, 20% of all economic crime is what we call "none of the above". I am starting at the bottom and working back, so "none of the above" shows that we have what I call an evolution cycle. Anything can be scammed. That is one thing that I was told when I came into this post last year. Having been here for six months, I can tell you that anything can become a fraud, depending on the context and the environment. What we see is a very quick turnaround of how crimes evolve; 20% of those are constantly evolving and we are constantly working with the emerging trends and trying to deal with those. Then 17% of crimes that we assess through Action Fraud are advanced-fee fraud. 14% relate to online shopping and auctions; 12% are cheque, plastic and online bank account fraud; and 8% is computer software and service fraud. That is the breakdown from what people tell us when they come and report those crimes to Action Fraud.

Q570 **Charlie Elphicke:** You said what people tell you. Do you think these are the most prevalent or are they just the ones that people report? Is there a difference between the two?

Karen Baxter: I would have to go through the notes but, largely speaking, they are the most prevalent. What we would do is we would look at those crimes but we have a control strategy that looks at all types of economic crime. We constantly review that and we look at the top 10.

We also look at what the risk of that crime is—the risk being the impact on the person—and the likelihood of that crime happening. That helps us to better understand the impact on the victim and also our response in terms of policing. That is, generally speaking, what we see as the most prevalent. You may want to come in on that.

Peter O'Doherty: They are definitely the most prevalent but these are the crime areas where there is realisable harm financially to the victim, where you have tangibly lost money. If I could give you a quick example that would not be obvious to a consumer, if you go on to an illegal website to download counterfeit music or films, a new trend that we have seen, very interestingly, is that the illegal advertising on that domain uses the CPU power of your mobile device to data-mine. It will do that through a million devices in order to achieve Bitcoin credits, for example. My father, who is very much new online, has not lost any money, and the computer power of his device, which is now much slower than before, is being used to fund the gains of an organised crime gang. Certainly, that would not be a crime that has been reported to us but, as soon as we find out about it, we work with the Intellectual Property Office, as part of BEIS, to share that information around to consumers.

Something else that we have done recently is that we have a proactive intelligence team, where we speak to offenders and say to them, "You are clearly very good at what you do. We would like you to tell us how you have done it", so that we capture it and share that advice with industry and consumers to help them protect themselves when using the internet.

Just to finish off, the challenge for us is how you reach 60 million people in the UK, all of whom have different experiences online. You have digital natives and Generation X who are born using the internet. They buy holidays online, university courses or homes. They use Bitcoin. You have people like my father, who only had a smart device last year. How do you give the advice that is relevant to different categories of people in a world where technology and globalisation is informing and changing the ways criminals exploit vulnerable people day in, day out? That is very much our challenge going forward.

Q571 **Charlie Elphicke:** Thank you for that. Commander, you have had an incredibly wide range of experience fighting just about every single crime there is, with your background in Northern Ireland, often with incredible innovation. From all that experience of fighting other sorts of crimes, what new techniques could we use to combat economic crime, from your own experience?

Karen Baxter: I was hoping you would ask me that question. I am going to go to the world of counterterrorism. Counterterrorism has a very visible impact on the public, on victims and on politicians; therefore, it gets a value in society—not a value that we all appreciate or we like, but it is a value—that allows it then to be prioritised. However, when you look

at fraud, in some ways the impact on victims is very much less visible, similar perhaps to domestic violence or to sexual crime.

What I would say is that the first thing is that the narrative needs to change around fraud. The impact, as you have said, on fraud victims can be massive. In fact, some people would say, "Take my life as opposed to leaving me to live through this". The first thing is the narrative needs to change. It is not the grey person's investigation or the grey person's crime. It has a very human impact and a long-term impact on the health and wellbeing of people.

The second thing is that, if we accept that, then we need to understand where it sits as a priority, not just for policing and law enforcement but for society, because it has a much stronger reach into not just the health and wellbeing of people but the health and wellbeing of this nation.

Thirdly, what I have learnt from counterterrorism is the power of intelligence development and the power of understanding the data. Going back to my first point, we are now at phase 2—the second iteration. We are now five or six years into this and we need to really grasp the data, understand it and move to a much more proactive stage.

What I would say is that, because of all that I have spoken about, fraud and economic crime has suffered from being the grey person's investigation. It is not seen as the edgy part of policing. For me and the team in City of London, along with the broader policing team, it is very much about now developing that into a more proactive type of investigation. That is critical. It is the key point to failure or success going forward.

What I have found is that there is an absolute willingness across our regional colleagues to come in and to do that. As part of the NECC, there is a willingness to do that. It is about using and exploiting that intelligence not just in policing and law enforcement but in banking. In order for us to do that, there are challenges around the sharing of information. I also see a willingness for us to do that but we need to work much harder around getting to the point where we perhaps respond in a way similar to the counterterrorism policing response.

Q572 **Charlie Elphicke:** Finally, these economic crimes often affect my constituents in Dover. They think they are buying something off eBay but it does not exist. They end up with push-payment frauds, people phoning them up and conning them out of their bank savings. These are massive issues but, from your experience, which of these crimes are most pernicious, regardless of economic loss?

Karen Baxter: I might refer to you, Pete, on the tactical approach. These crimes have cycles. What we see are emerging trends. We see certain things will trend at certain times. The benefits of having a national lead force and central co-ordination is that we understand where those trends can start to emerge. We can also respond to those much more

quickly. When we see a trend emerging, we can very quickly get there online and try to engage with people to prevent further crimes happening.

Peter O'Doherty: The financial loss to any person is unacceptable. The question is not just about how much money a person has lost and the impact it has on the sustainability of a business or on a person enjoying their pension, for example; it is where the money goes. They are all pernicious because we know for a fact that a lot of that money, whether it stays within the UK or leaves the UK's shores, is clearly used to fund all aspects of serious and organised crime, ranging from terrorist fundraising, through human trafficking, to the importation of drugs and firearms. There are two parts: it is about people having a financial loss in the first place, and what it then does is it affects people's confidence to use the internet or to speak to family on Skype. When BT rings at the door, you start to question, "Is that really BT?" and you start to have a lack of trust in anyone and everything.

There is a specific trend. In most of the economic crimes that we see, they do target vulnerable people. In some cases, you can buy lists of vulnerable people on the dark web. There are other ways to target vulnerable people. Invariably, these people are alone and have very little money. Once that money is taken, when you look at the response from policing, which is improving but is not perhaps where we would like it to be, it is a big risk.

I would just say that Government, over the last few years, have invested, are investing and will invest more and more around the economic crime capabilities at a local, regional and national level. However, the reality is that, if any of you, heaven forbid, go to a cash machine and take out £50, and you are assaulted and that money is taken from you, the police will always investigate. If you go online and buy a holiday for £5,000 but, when you get to Gatwick airport there are no flights and no hotel, who is going to investigate that? Like the Commander says, that narrative does need to change.

Just to finish off, something that I am very proud of around UK policing is democratic accountability. Quite rightly, Sir Robert Peel said the community is the police, and the police is the community. What should shape the priorities in which we provide local service is what the public wants, but the reality is that, when you go to your local communities and ask the public, "What do you want the police to do?" they mention antisocial behaviour, feral youths, littering or dog fouling. These are important issues but there is a gap between the strategic threat and risk assessment and what our local people want. There has to be a compromise whereby the police improve their ability to educate people and to work with the public to influence them about what really matters here. Cybercrime and economic crime is a big problem once you have been victimised but, up until that point, for an average person, it is a fairly invisible crime.

The last point is that we have this struggle in Action Fraud. If I could give you a very quick scenario, imagine it is four o'clock on a Friday afternoon and I have two crimes in through Action Fraud. The first crime is Mrs Higgins of 1 Acacia Avenue, who has lost £5,000. She has nowhere to turn and she is vulnerable. She has lost her pension. The second attack is a state-owned bank that loses £500 million in a network intrusion. If I could only investigate one crime, which one would I investigate? It is an impossible question to answer because, if the state-owned bank loses £500 million, all of our insurance premiums go up, so we all lose. Trying to find that balance is the challenge for us going forward. There are a few challenges.

Q573 **Chair:** Just before I hand over to Catherine, what you mentioned earlier on about data-mining was fascinating. When you get the people and you are able to ask them how they did it, do they tell you?

Peter O'Doherty: Interestingly, trying to find the bad boys and girls behind cryptocurrency fraud is challenging. I will give you one quick example. It is no secret that what policing love to do is to catch the bad boys and girls before they come to our attention. Typically, if you go on to the dark web, you can buy drugs and firearms, and then catch people out. It is no secret that the police do this.

What is really difficult is that, on the dark web, back in the day, you could use a covert identity. Now, however, most of the dark web vendors only accept Bitcoin. They exploit a range of cryptocurrency platforms, so that you can never trace their identity. For example, if you data-mine, it is published on Blockchain, which is an accessible document. A very good IT-literate person could trace the source of that transaction, but criminals are finding their way around it, so that tracing that source is really challenging, plus you have vendors who operate from hard-to-reach jurisdictions and territories where the diplomatic relationships between the UK Government and these jurisdictions are perhaps not where we would like them to be, so providing an investigative response is very challenging indeed.

Karen Baxter: Could I please come in? You raised a really interesting point: do they speak to us? Do they tell us? If we look at serious and organised crime legislation that allows people to work with the Crown Prosecution Service, coming out of organised crime gangs—we call it SOCPA legislation—one of the areas that we need to get to is exactly what you talk about. In terms of counterterrorism and other serious crime, we naturally look at trying to get people to come out and give evidence against those who are causing the most harm.

In order for us to do that, there is something around us needing either strong deterrence or a strong incentivisation. There is a disparity. There are differences in sentencing between the United States and the United Kingdom. That is probably a debate for beyond this room. However, one thing that there is a sense of, anecdotally or otherwise, is that the stronger sentencing in the United States may be an incentivisation for

people to come and work and co-operate with law enforcement. That is significant when you want to break into criminal networks. It is also significant if you want to deal with criminal enablers such as solicitors, professionals or accountants who enable the money laundering and the washing of dirty money through the system.

Q574 **Catherine McKinnell:** We have heard that it is difficult to get an idea of the scale of consumer-facing economic crime. One of the challenges is that it is not consistently reported. Some people go and tell their banks; other people will tell their local police; other people will report it to Action Fraud. Could you, first, just outline what the right course of action is for a consumer who either suspects or knows that they have been a victim of this crime?

Karen Baxter: It is one area where we are working with our partners in law enforcement and also in the private sector, so that whoever the victim is, they will come to an organisation and whatever information they provide then populates all of our databases so that it can be used. That is important because it causes less distress for the victim. It allows them to populate and give information once and for us to use it multiple times.

However, in terms of how they should act today, if there is a crime in action or if you see money leaving your account and you want immediate attention, it is the 999 system. We would encourage anybody just to phone 999 and get that assistance straightaway. If you see that there are issues with your debit or credit cards, what we would suggest is that you can contact your bank and they will give you the immediate assistance that you would need to block those cards. What we would also then say is that, having taken those immediate steps to stop the harm, you would then contact Action Fraud and make that report.

There are occasions where people go to local police stations and they can make their report there, but then they would follow that through with a report to Action Fraud. The benefit of having that central reporting system, which is very much the envy of other countries and other law enforcement, is that, while it is not perfect, it allows us to start to mine and bring all of that data together. It allows us to use the intelligence and to understand the offending types. I would always encourage people to stop the harm first of all—999 or contact your banks—and then immediately contact Action Fraud.

Q575 **Catherine McKinnell:** That is down to the individual to do that. That is what individuals need to understand. Is that correct? This is not necessarily advice they are getting from their local police or from their bank.

Karen Baxter: The advice is well signposted out there. Certainly, banks will explain that to victims. It is also very well signposted online. Local police will also advise people to do that. In fairness, it is reasonably well signposted for people to do that. In the first instance, if people phone the

police, they will then refer the matter through to Action Fraud. From that perspective, people will get the help by contacting the police in the first instance.

Q576 **Catherine McKinnell:** Would it not be appropriate to make it incumbent on the banks to report fraud that they have processed, dealt with or intervened in and, once they have stopped the harm, then report it as a crime rather than leaving it to the individual, who may or may not then take that follow-up action?

Karen Baxter: I am going to come to Peter in a moment. I have a couple of things to add. There is the legislative requirement of the banks under SARs to contact us if there are issues and challenges around an account. Frequently, the banks do contact us. We have had some very successful jobs recently where we have had the banks contact us because of information that they have seen through their systems. That is where we need to get to more in the future, where we are looking at the crimes in action, where the fraud is taking place and we can much more quickly start to make interventions around that. That is about sharing information at the appropriate time and at the earliest opportunity. In fairness, the banks do that.

Q577 **Catherine McKinnell:** Not always though. Not in every case.

Karen Baxter: Not always. I am trying to be devil's advocate here and I would like that information from the banks on every occasion. What I am told is that, because the reimbursement has happened and because of the bureaucracy that it would take to inform us, there is another debate on that. Would I like them to contact us? Yes, I would. Would I like that information and intelligence? Yes, I would. Could we use that going forward? Absolutely. You make a fair point. The other aspect around the bureaucracy and the finance behind that is something for the banks.

Q578 **Catherine McKinnell:** I would be delighted to hear from you as well, Detective Chief Superintendent. In terms of responsibility for collating that data and your confidence that it is currently accurate and reflects the full scale of this crime, how confident are you and who has that responsibility? Who is officially responsible for collecting that data?

Karen Baxter: We have a responsibility, on the Action Fraud side of things, to collate an enormous amount of information. At this moment in time, I know that people in banks and the financial sector will also collate an enormous amount of very valuable information and intelligence. There are responsibilities right across law enforcement, public and private, around who collects the information. For us, going forward, the secret—and I am reluctant to say "the golden nugget"—is how we unlock that so that we can have a free flow of information with due diligence such that, when we need information quickly, we can move forward. It is important that each respective organisation gathers the information and quality-checks that information, but also proactively looks at where that

information should be shared in order that we prevent fraud going forward. That is the first thing.

In terms of how we quality-check it and understand it, we accept that a large amount of fraud is not reported, for a variety of reasons, and therefore there is an unknown to this. That is why we encourage victims to come forward, because they would potentially have crucial pieces of information that would allow us to be better informed around threats today and in the future. That then allows us to respond better. There are two aspects to that.

Q579 **Catherine McKinnell:** Detective Chief Superintendent, did you have something to add?

Peter O'Doherty: Yes. "Pete" is fine, if that is acceptable to everyone.

Just to clarify, this has been a topic for discussion around Government and policing for a few years now. The Home Office counting rules govern how we record and process crime. They say that, if you are a victim of a credit card fraud—which, sadly, most people are at some point in their life—you phone the bank. What normally happens is your bank reimburses your money and then investigates. Under the Home Office counting rules, at the moment you are given the money back, the bank becomes a victim and you are no longer the loser.

What then happens is that some banks do not always report those crimes. What do we do to get around it? There are two things. The first is that we have UK Finance, which is effectively the trade body for retail, private wealth and corporate banking. They report in bulk, every week, those crimes into our system. What we do is we wash those crimes against the crimes from people and businesses through Action Fraud to create big cases that policing can investigate when we send them out. What you can do is, once you have the money back from your bank and the bank now becomes a victim, even though you do not report that crime as a bank, the original victim—the citizen—can still report that information to Action Fraud. That information is then used to understand how it happened, so we can give the right advice out.

Just to answer your question, we get the crimes in from the trade association but it is certainly not all of the crimes that affect each and every citizen.

Q580 **Catherine McKinnell:** Do you think that banks and financial institutions are incentivised not to report all crimes? Do you think they have an interest in or a concern sometimes about reporting the actual level of crime that they experience or that their customers experience? In terms of the other side to that, do you think that banks are doing enough to encourage victims or their customers to individually report those crimes?

Peter O'Doherty: I have worked in the economic crime space for the best part of seven years. When I compare the response from financial institutions back in 2010 to where we are now, there is a significant

improvement. Banks take very seriously supporting consumers. If you look at the devices that you can now use in online banking, from secure apps to biometric devices, they are taking this seriously.

In terms of your question around why they do or do not report, I have never worked in banking before and it is perhaps not for me to say. What I would say is that it could be a combination of a number of things, ranging from high volume, being realistic about whether an investigation will ensue from local, regional or national policing, whether it costs more to report as opposed to—

Catherine McKinnell: Dealing with it.

Peter O'Doherty: Yes. It is perhaps myriad things but what I would say is that we have a very good relationship with banking. They are very supportive and doing more than they have ever done before.

Q581 **Catherine McKinnell:** Overall, my concern is that, if we do not have the full picture of this economic crime, how do we know that we are addressing it sufficiently? How do we know that we are resourcing the ability to police it sufficiently? Presumably, they are concerns that you would share.

Karen Baxter: It is a really valuable point in that we have a really good picture. We have not done what I call the iteration—the phase 2—in terms of really starting to interrogate the systems. We do not have a lack of data; what we have is blockages in how we pool the data from each respective part of law enforcement and private, how we pool those in a very mature way, and pool that information and match that together.

I do not need to bring out all of the banking data. I do not need to go to my partner law enforcement and get their data. What I need is for each and every reporting organisation to start to make sense and interrogate the data. At the National Economic Crime Centre level, or perhaps even at a tactical level below that, we need to start to cross that over and understand it. It is the 80/20 Pareto analysis. We talk about 800,000 contacts to Action Fraud. We do not have, I would suggest, 800,000 fraudsters. We do not have that amount of people—I hope not. However, what we have is a core of people who will commit 80% of the crime and the harm. Our secret and our challenge going forward—and we are absolutely up for this—is how we pull that together and get the picture of who the 20% are. We all need to put our assets towards this—public and private sector working together.

For us, I would say that we have loads of data. We will encourage and welcome more people to give us more of that, but we now need to analyse and pull that together into a meaningful picture.

Q582 **Catherine McKinnell:** On that basis, I know that Christmas is over but what is the one thing that Government could do that would assist you in that endeavour or in your work?

Karen Baxter: Probably one thing is around that facilitation of data sharing. It is a facilitation that we need. In terms of GDPR, sometimes people say, "Has it slowed stuff?" or "Has it stopped stuff?" GDPR has just put a framework around that. The first thing that I would say is that we all should be responsible when we manage other people's data and personal information. In that respect, GDPR is fine. Perhaps it has slowed, in some cases, the exchange of that information.

Going forward, if you take where we were in counterterrorism and the value that we put in fraud, we probably need to be a bit more audacious in testing some of that legislation. You yourselves are a very influential group around opening up the debate. There is always a debate around the protection of the private information that we all have and that we do not necessarily wish to share, but it is about how it is necessary to share that information in the bigger scale of how we then protect the nation as a whole and how we protect the population, and particularly those most vulnerable.

The debate is somewhere that we need to start to open up, and that then impacts on the narrative. It impacts on how we share information. It also impacts on how we more effectively use that information. For me, in the first instance, it is the discussion here. I am going to take two: it is about the narrative and the discussion, and then I would say it is about how we share that in the most efficient and effective way.

Peter O'Doherty: I would just say, if I may, one thing on a more technical level. A lot of the crimes that we prepare and then send out to law enforcement for investigation inevitably include a bank account. As part of that process, we want to make it as quick as possible between you reporting a crime and getting an investigation. We have to go to the plethora of banks and get a Data Protection Act request, where, effectively, we are looking for the owner of that bank account as a significant, if not the main, line of investigative inquiry. The ways in which the banks respond to that are different: some are very fast and some are not. They have different prioritisation systems. Something that we have been discussing recently is the possibility of a central registration of bank accounts, where, in real time, we can access this platform of registered bank accounts, which will make our process so much more expedient and efficient in getting an investigation for every victim who makes that report. That would be really key for us.

Just lastly, to finish for me, there are a few initiatives. We have the Joint Fraud Taskforce at the moment, which is an initiative between Government, law enforcement and banking around sharing trends and typologies, trying to look at how we can improve the sharing of information and intelligence and the identification of organised crime groups, so that we have a collective response across Government, the sector and policing. We have also had in the past—and continue to have—members of the banking sector working within Action Fraud and the National Fraud Intelligence Bureau—NFIB—where effectively they are

looking at the data that they are seeing and the data that we are seeing, and washing it together to find commonality and to find threats, trends, typologies and people who are committing these offences, so we can collectively have an intelligence-led response to the prevention, disruption and enforcement of those people.

Q583 **Alison McGovern:** That is very helpful information. I just want to come back to the impacts on consumers, because some of the evidence that we have heard is quite disturbing in terms of fraudsters targeting elderly people. It is certainly reflected in my constituency caseload that it is people who are less likely to be IT literate who might be vulnerable for some other reason. Which?, the consumer organisation, also told our Committee that there is a trend for people to be called late in the evening. People get the call on a Friday night and are persuaded into transferring funds because, if they then report it, it is less likely for there to be anybody around to deal with it at the bank. Could you just talk about, from the consumer's point of view, the particular trends that you are seeing? What have you identified in terms of trends?

Peter O'Doherty: They do everything and anything, so, yes, absolutely. They target people late at night when perhaps they have been working all day and they are tired and more susceptible. They are targeting people who have just recently opened up an email address. They are targeting people who perhaps have significant disabilities or vulnerabilities. Sadly, a lot of that information is available in different places. You can access that information on the dark web. You can access that information from people's home computers through the deployment of malware and anti-viruses. For example, if you get an email that says, "Cheap flights to New York for £200" and you open the email, it can put a banking Trojan on your machine, so that, every time you do online banking, it effectively fills your user name and password. It will do it a thousand times, send it to a cloud and sell it on the dark web, and it goes on and on. There are different ways to access the information.

To your question around trends, there are many. For example, as the Commander was saying before, computer service software fraud is a big issue. This is where you will get a phone call, normally from Indian call centres, which say, "Hi, we believe that you use a Microsoft product and we are here to give you a free upgrade". What they are doing is using a remote key-logging device, accessing your computer via the internet and effectively taking control of your machine. They normally put a virus on your machine, so that, every time you use social media or online banking, it is recording all your personal information. It does not matter if you are a young person really familiar with the internet or if you are an elderly person. It is easy to understand how you can be vulnerable to that crime type.

In terms of advanced fee fraud, we see students and younger people who are not financially well-off being targeted easily. How that fraud works is that, invariably, I will contact you to say, "I am a rich entrepreneur" or "I

have won the lottery. I have won $100 million and I need you to store the money for me while I move to the UK and cash out my savings. I am going to give you £10,000 as a bonus payment. I just need your bank account details, so I can give you the £10,000". People believe something that is too good to be true, and the money is gone.

In terms of online dating fraud, what happens here is lonely people—perhaps people who are elderly, single or divorced—will create an account on a dating website on a one-month trial. They will befriend someone who purports to be a very attractive female, normally. They build up a relationship and the person believes, "Oh my God, someone does really love me and this is amazing. They like the same things as I do. The formula in the website basically says that we match perfectly. But now they want £20,000 to buy a flight and get to England so we can have our first date".

Cheque, plastic card and online bank account fraud can happen to anyone and everyone. People always wonder, "How did that person get my credit card details?" Everyone says, "It must have been the waiter in the restaurant". It really was not. It was the email that you opened. It was the website you looked at. It was the malware on your machine. It was the theft of your personal information. It is done a million times, and that is how most of us will lose money on our credit card, for example.

It happens to everyone. The biggest vulnerabilities are people who are not comfortable living their lives online, and people who are very new to that way of living. These are definitely most commonly the people we see.

Q584 **Alison McGovern:** It is basically over-confidence and lack of awareness, as in a group who are over-confident because their whole life is online and they just do not take enough care, and then there are people who do not have enough awareness of the risk because they are new to it.

Peter O'Doherty: Yes. I will give you a quick example. One of the common frauds we see are popular businesses, like supermarkets and banks, where an offender or a crime group will create a website that looks exactly the same. Instead of an "l" it has a "1" or, instead of an "O" it has a "0". Thousands of people will go online to use the internet to do their home shopping or online banking. What we find is young people who are born and raised using the internet will look at the website more closely. They will make sure that, when they make a payment, they see "https" and the padlock in the URL. If the website is a British company and the English is really poor, they will ask, "Why is that English so bad?" They will go online and look at Whois. They will ask, "Why is a British company's website being hosted from Ukraine?" They have that confidence, as you say, and that experience to use some simple tools and techniques to do that.

However, someone who is very new to the internet is so overwhelmed by the options on the webpage and how it all works that they are just

blinded by it. It is like using a car. Any of us who own a car will make sure that, if the car is older than three years, it has an MOT. You have to wear a seatbelt. You have insurance. It is about having that mindset online. For policing, this is really hard. Back in the day, for a bobby on the beat, crime prevention was going to someone's house for a burglary and saying, "You need to have double-glazed windows. You need to have an appropriate lock and key". Now prevention advice means a bobby on the beat going into your home, looking at your machine and saying, "You need a firewall and an anti-virus platform. You need to apply parental controls". That whole narrative and style of policing has to change to protect those vulnerable people.

Karen Baxter: We are talking a lot about vulnerable people, and there is a risk. To go back to the narrative, what I have had said to me is, "Surely, fraud is only committed against those people who are vulnerable" or, in brackets, if you do not mind, "stupid people". Can I tell you: it is not stupid people and it is not entirely vulnerable people? People find themselves vulnerable because of a whole range of factors. People can be vulnerable at certain times in their lives and not at other times. Fraudsters are like criminals. They are very smart. They will spend months grooming a certain type of crime type.

We had an example of the Grenfell Tower disaster and a fake charity website. We all understand and we recall the emotion of the nation at that stage, and how we all felt when we saw those images. We think about the fraudster. The fraudster knows all of that. The fraudster knows exactly how we feel. The fraudster knows that there will be quite a large number of people who will want to do something about that. The fraudster grooms people. They look at the emotions. They understand the psyche of an individual.

That is why, when they look at older people, 30% of older people will be more subject to advance-fee fraud. There will be certain types of fraud which might go towards the 60-69 age group, which is the dominant age range for dating. That is significantly more than the 70-79 age group. Some of that is because people have a disposable income. They have worked really hard. They have retired and they have a disposable income, and yet they perhaps find themselves a little bit lonely or perhaps they just think, "I want something different in life". There is a balance to be had around the fact that not all people who are victims of fraud are vulnerable; indeed, many are not.

Q585 **Alison McGovern:** Just finally, we noticed the City of London Police putting some information into the public domain about fake car insurance. Is this an emerging trend that we should be aware of?

Karen Baxter: I do not know if it is an emerging trend. It has always been there. We have had ghost brokers: people not only in car insurance but any types of insurance who will purport to be insurance providers. They will take your money and provide you with certain documentation. Unfortunately, when you need to rely on that documentation, what you

will find is that it is null and void. We have a specialist part of our organisation that we call the IFED unit. IFED works with the insurance industry and, in exactly the same way generically as fraud, we are looking at lower levels in terms of the amount but we have opportunistic types of fraud on a regular basis through the auspices of insurance.

The benefit for us of working with the Insurance Fraud Enforcement Department is that we work with insurance companies throughout the United Kingdom. We can start to get the information. We trend it and look at where the emerging threats are. We can also then put out information that protects people from being a victim going forward. That is a valuable piece of work. Everybody in the United Kingdom pays around £50 extra for their insurance, so—back to the narrative—this costs everybody and we all pay for this.

Q586 **Wes Streeting:** Good morning. I want to return to this issue of reporting fraud and, in particular, the role of Action Fraud and the role of banks. We have heard evidence from consumers that they are told to report to Action Fraud, but Action Fraud only collates data and then passes on some information to local police forces. That is something that has been re-emphasised this morning. The reporting of the economic crime to someone who is able to investigate what happened appears to be delayed in some cases. I just wondered what benefit you think Action Fraud brings to victims or to the police.

Karen Baxter: I will let Pete come in but I will say a few things first of all. The first thing—and we have said it a few times today—is that having one central co-ordinating point where everybody can report that information to is the envy of law enforcement in many other countries in the world. That is the first thing.

The second thing is that, yes, we admit that it is not where we wish to be and we are constantly evolving and moving forward to improve that for the victim and for the journey that they unfortunately find themselves upon. What we have done recently is that we have been working over the last few years to develop new systems. Those new systems will help us to interrogate the information better and more quickly. When we have that information, it allows us to respond in a more efficient and effective way. We will also work with that new system—and we are working with 43 forces and ROCUs at the moment—to ensure that the information we have becomes more transparent and more available to those forces. That is about expediting how we get cases out to forces and also the information that they have to allow them to act more effectively and at an earlier opportunity. What that, we hope, will do is allow them to gather evidence at an earlier stage.

What we are trying to do here is we are trying to improve the whole system of law enforcement, of evidence gathering and of developing those lines of inquiry at the earliest possible stage. When you have a national reporting system, it allows you to understand the problem. The difficulty, if you do not have that system, is that you have victims

phoning 43 different forces with a disparate and ad hoc type of response. What I would guarantee you is that, no matter how much effort I put into that as a national coordinator or as a national lead force, if we had that system with 43 different responses, I would suggest that we would not have the data that we have now. Therefore, we are taking ourselves back about 10, 15 or 20 years.

What we need to do is to ensure that the system is strong, that we have a resilient and robust mechanism whereby we provide the best service to victims and, at the same time, that we have the systems that we can interrogate and turn into really strong investigative packages. A national reporting system is absolutely key in the fight against economic crime, and the next stage is about now moving to how we develop that intelligence.

Finally, before I move to Pete, I would say that it is not just about the intelligence and policing, but about broader law enforcement and our partners. That is critical. Going back to your point, it is about really, truly understanding the threat and the risk that we are dealing with here in 2019.

Peter O'Doherty: I would echo everything the Commander said. I would just say that, before Action Fraud, it was very much a postcode lottery. Fraud had never been a local priority for policing. Since the inception of Action Fraud, it has made an invisible problem very visible. If you consider a fraudster who, let us say, travels across the 10 regions in the UK and commits 10 crimes, even if those 10 regional police forces had investigated that person, you would have had 10 concurrent investigations targeting the same individual, which is incredibly expensive. As the Commander said, having a central repository helps you understand what the trends and typologies are. Once you understand what those are, you can understand what capabilities policing needs to investigate those crimes, and it helps us understand how we can prevent them and have other avenues for justice, such as disrupting the platforms that create repeat victimisation, like websites and bank accounts. It helps us understand the training that we have to provide the law enforcement industry. We have our Economic Crime Academy that looks at what we get into Action Fraud. It looks at the capabilities of the police to investigate these crimes and works out what else we can do to upskill detectives and investigators to provide more investigations to victims.

Q587 **Wes Streeting:** You have made a clear and compelling case for the centralisation of some of these activities, such as the collation of data, the oversight, the intelligence sharing and the investigation of patterns of economic crime to try to catch people who are responsible for perpetrating it. Where I am unclear about the benefit of Action Fraud is to individual victims of crime. The Committee has been given an example of where someone reported a fraud to Action Fraud, the information was not passed on for three months, and then the information was lost, so they

had to provide the details again, so a stressful experience was made more stressful.

I appreciate that we all see individual examples of things going wrong that do not necessarily point to an endemic problem, but it does also chime unhappily with the experiences of one of my constituents, who was a victim of ID theft. Someone had taken out a loan for £42,000. They reported it to the police and to the bank. The police suggested they also report it to Action Fraud, which they did. The problem was that the expectation was created that there would be a response from Action Fraud and that it would lead to investigation and updates, and so they were left feeling failed by a service that they were expecting. It seems, from what you have told the Committee this morning, that it is an expectation that ought not to have been given to them. When I wrote to Action Fraud, it took two months to receive a reply, which I found unsatisfactory. At the end of it, the constituent finds out it is an information report and nothing else is really going to happen as a result of it.

I understand, following that, that the Action Fraud website was updated to better signpost and advise people about what Action Fraud really does. I know that from first-hand experience, when I was a victim of identity theft. My reaction to reading your website and being asked to fill out a whole number of cases for each and every example of fraud that was perpetrated against me was that I just thought, "What is the point? This is as useful as a chocolate teapot to me because you are not necessarily going to investigate my case or provide an outcome". I understand why the data and the intelligence gathering is useful to you, but why are we giving the victims of crime the run-around? Surely, it should be the banks and local police forces that report in. Why are we putting this onus on the victim, when they are unlikely to see any positive result from reporting to Action Fraud?

Karen Baxter: The first thing I would say is that the case you discussed is really regrettable and I am sorry about that, because no victim should have to be in that position. That is what we want to move away from. We want to reduce and eliminate those types of experiences. We will not be able to eliminate those types of experiences if we do not understand what we are dealing with and if we do not understand what we are dealing with in the future. Therefore, I would say that, despite the challenges that you have experienced and despite the challenges that victims do experience, the information that you have is critical. It is absolutely essential that we get that information because then we understand what we need to be doing, how we need to grow and how we need to respond in the future.

They may sound like hollow words to you but what I can reassure you is that the information that we have gathered over the last five or six years has enabled us to provide a better investigative response. The development of, for example, specialist units that work with the banks and with insurance has allowed us to bring people to justice earlier and more effectively. We would not be in that position if we did not have what

you call the intelligence. People do not entirely appreciate the intelligence aspect of that. Not all information can be acted upon in terms of a prosecution, but it is incumbent upon us as policing to take that information and say, "How do we learn from that?"

Every single day at the moment, we are looking at what victims tell us. In fact, we had a conversation this morning around how we provide that better response at the front end. At the moment, we cannot get in touch with victims as quickly as we would like. We had a conversation—this is part of our everyday work—around how we maximise the money that we get, how we increase the resources that we have and how we make that impact better, and not only for policing. In fact, policing is the afterthought. It is about how we improve how we support you as a victim. That is very much critical to how we improve that victim journey.

The second thing is that whether you get an investigation or not is not always with the national lead force, NFIB and Action Fraud. What we do is we bring all that information together. A significant proportion of those investigations will go out to forces. You quoted a situation where it did not go out for a number of months. If I can explain to you why, perhaps, some of those cases did not go out for a number of months, in some cases we have volume. We have 800,000 contacts a year. That is going to take a certain amount of time. With a finite budget and resources, there will be an element of that and we will have some degree of backlog, so we are not where we wish to be in terms of how quickly we get crimes out the door.

The second thing is we look at it in terms of whether that crime is able to be investigated and, if it is and if there is any sense that there is a line of inquiry there, we will take that and we will ask the banks for information. As Pete has already said, we have varying degrees of efficiency from respective banks, so, in some cases, the delay in getting cases out to forces has been the delay in getting the information from the banks. What we have just recently done is we have reviewed that process. We are looking at how we engage better with 43 forces, give them the information they need in a quicker way, and apply for the information from the banks. We are also working with UK Finance to see if we can expedite the slower banks to assist us. If we can shorten that cycle, we provide them with the opportunities to help us. What does that do at the end of the day? It improves the outcomes for victims, not just in terms of pursue but in terms of prevention for the future.

What you talk about is a really complex situation. I am not going to patronise you and tell you that that was just a one-off. There are, unfortunately, cases like that, but what I would like to do is give you the reassurance that it is first and foremost in our minds. As the national lead force, it is one area that we are seeking to very much improve. That is part of the reason why we follow up with things like economic crime victim support units. We are working with that. We are working with

regions to try to establish that and roll that type of support out even further.

Q588 **Wes Streeting:** First, thank you for your apology, which I will pass on to my constituents. Sincere apologies are never hollow or unappreciated. The candour with which you have addressed some of the structural, process and resource issues will also be really welcome to them as well and they can see that these are issues that you have identified and are working on, so I appreciate that.

Finally, on this issue of banks reporting to you, what can be done to improve this? Can I invite you to help the Committee to encourage some of the core culprits to improve their game, by telling us who they are? Do not worry; we will not tell anyone. There is a serious point here because, listening to what you have said, one of the reasons why I did not bother to sit on your website and do all eight examples of credit cards and bank accounts opened in my name was because it was a bit laborious and I thought, "What is the point?" What concerns me even more, listening to your answer, is that my time doing that may well be well spent because negligent banks are not bothering to do it on our behalf. I would be curious to know, as a consumer, because my notes about which banks were useless at dealing with my experience as a victim might well correlate with your experience about which banks are useless at reporting to the police.

Karen Baxter: The Home Office was trying to develop a central register of good banks and not-so-good banks. That is for a whole other debate.

Wes Streeting: We will go and ask them.

Karen Baxter: There is something around that. Inevitably, there are such banks. We work with UK Finance and we have a very strong, positive relationship with them. We met with them right before Christmas. We raised those issues and they will work and are continuing to work to ensure that the timescales that we work to are much more efficient. There are certain aspects of this. Challenge is good. It is constructive and should not be feared. Things like this—good, strong accountability and transparency—are what are needed. Across not just law enforcement but the banking sector, it is to be welcomed as well. What it does is it makes everybody in every organisation personally responsible for changing where we are in 2019. I am not going to give you a league table—I will leave that to my banking colleagues—but what we have done is we have raised, in specific cases with UK Finance, good practice and bad practice. What was explained to us was that their view is that they will go and try to disseminate some of the better practice and understanding that perhaps some of the better banks have with those banks that maybe are not as efficient. In the first instance, that is to be welcomed.

Wes Streeting: It might be helpful if you could write to the Committee with the good practice and the bad practice, not necessarily naming the

banks. That would be very helpful for our report and recommendations. Thank you.

Chair: UK Finance can be assured that we will be calling them as part of this inquiry. They have already been in as part of it but they will be coming back.

Wes Streeting: Their public affairs officer is going to be delighted.

Q589 **Colin Clark:** The Committee has heard evidence that the police do not investigate if the total loss by an individual is under £100,000. Pete, you mentioned earlier that you need to make judgments on this. However, we have also had written evidence that the police were helpful in a case where the loss was half that amount. What I am trying to clarify is whether there is a minimum amount below which it is unlikely that a crime will be investigated in this space.

Peter O'Doherty: Again, this is such an important issue. With so much demand coming in, we apply a range of measures to understand what crimes we are going to develop and send out for investigation. To answer your first question, no, it absolutely is not the case that we only develop crimes and send them out for investigation where the reported loss is over £100,000—absolutely not. However, of all the different measures we apply, one category we always look at is where the reported loss is £100,000, but that does not mean that crimes where the reported loss is much lower do not get looked at. That is absolutely not the case.

We look at the threat, harm and risk of each crime, at the reported loss, at the vulnerability of the victim and, most importantly, at the availability of lines of investigative inquiry, so we know that, with some development, we can absolutely find the offender and bring them to justice. These are some of many ranges of measures that we apply to decide what crimes we are going to take off that queue, develop and send out for investigation.

Q590 **Colin Clark:** Are you able to do it the other way round? One individual is robbed of £5,000 as opposed to £100,000 but if one fraudster has robbed several hundred thousand pounds, are you able to weight it the other way and go after the fraudster who is repeatedly and constantly doing it? Is it possible to identify that?

Peter O'Doherty: Absolutely. One of the flags, if you will, is what we call a linked serious crime. Where there are multiple victims who have been victimised in relation to one type of crime, then absolutely that is one of the triggers for us for urgently looking at those crimes, developing them and sending them out for investigation.

Q591 **Colin Clark:** I want to move on a little bit but I want to phrase it a little bit differently. Again, Pete, you made the comparison between being robbed at a cash machine and online fraud. One that we have heard an awful lot about is authorised push-payment. *The Sunday Times* did an article last year saying somebody armed just with a fake ID stole £74,000. In September last year, the banks announced a voluntary code

to try to help unauthorised push-payment.

Are we doing this the wrong way round? If I use your analogy of the cash machine, you are limited to what you can take out of a cash machine, but a victim who came to me, not as a constituent, was robbed of several thousand pounds in one day by repeatedly going back to the bank and taking out £1,000 in cash. We have had evidence given to us of an enormous amount: over a week, somebody was robbed of £300,000. Have we got this the wrong way round? If the perception is that smaller amounts will not particularly be investigated—and that is not a criticism of you; I have read in the notes that it would be too expensive to pursue it—have we not got this the wrong way round? Should we not be asking the banks to realise that banking has changed and that, if there is a £200 limit on a cash machine, why is there not an absolute limit? I know that private individuals will not like this but the reality is that they can be robbed of vast amounts.

In the evidence, Commander, that you have been getting from your working with the banks, we are asking you to clean up the mess, but have we got it the wrong way round? Should this not be possible in the first place? Do we need the same sort of limit that we have on cash machines?

Karen Baxter: Those are all really interesting points for debate. If you look at 2019, everybody wants the ease of money payment and the ease of access to their bank accounts. You open up your phone, you press the phone and there it is; your bank account is there. You can make a payment. We can all make a payment. We are really used to that now. There is part of a much broader debate around what society wants. Is it the ease of payment? Is it the fastness or do they want to reintroduce levels of safety and security? For me, that is a much broader societal issue. I do not disagree that by putting those mechanisms in, it certainly slows things down.

Q592 **Colin Clark:** Authorised push-payment, Commander, is almost an old-fashioned crime: the idea that you ring somebody up at the end of the day, when, you say, they are feeling vulnerable. Interestingly, the person I spoke to was a very sophisticated person and managed to be robbed of a large amount of money by simply taking it out of the same bank repeatedly. At no point did the bank say, "What are you doing?" It is old-fashioned crime. It is like standing at a cash machine and saying, "Take out more money and just keep giving it to me".

Karen Baxter: You are absolutely right. One of the areas that we have developed in recent years with the Joint Fraud Taskforce has been the Banking Protocol. In terms of the Banking Protocol, that is about raising awareness with banking staff and also with police officers right across the country. Where we have really made an impact in that is where you have people who are coming in and doing exactly that, where you have them coming in and making repeated withdrawals. One withdrawal looks okay, but the second and third withdrawals start to look unusual.

Colin Clark: Or six.

Karen Baxter: Exactly, and also particularly if you are standing with some strange individual in the background. The Banking Protocol has been a really good piece of work that has saved quite a significant amount. We have had 369 arrests as a result of that, and we have prevented £40 million from going out into the hands of criminals. It is a really simple way where multiple organisations got together through the Joint Fraud Taskforce and we said, "Here is an issue". Does it eliminate it? No, it may not eliminate it, but certainly what we have is bank staff now at the front desks much more aware of, "Karen Baxter comes in. She usually lifts £50 a week but she suddenly comes in and lifts £1,000". We now have systems in place that look out for that actively and start to try to take measures to prevent that, which is only to be celebrated, in many ways—that we have managed to reduce that crime in some way.

Q593 **Colin Clark:** It is for this Committee to pull together the evidence we hear to make recommendations, and I just feel we are asking you to do a tremendous job, which you are doing, but to sort out a mess where our regulation has not caught up with the technology of our banking. As you said, people think this is a vulnerable crime and that these are victims who are, to use the word, "stupid", but of course they are not. This is happening to lots of people, and people do not want to announce it publicly.

Chair: Do you have a final question?

Q594 **Colin Clark:** Yes. Sorry, Chair. I am just diving off into different subjects. What is the biggest barrier to a successful investigation and what could be done to improve the situation?

Karen Baxter: Do you only want one biggest barrier?

Colin Clark: You can give us a few, but I will get it in the neck from the Chair.

Karen Baxter: There are a few barriers. Very quickly, it would be remiss of me not to talk about disclosure. In terms of disclosure, not just here in economic crime but also in all other types of serious and particularly complex investigations, we currently have cases where disclosure extends to well over 70 million pages. If you think that 70 million pages take about six months to establish, develop and check, there is a massive amount of work in ensuring that we meet the disclosure levels. Criminals know that and, therefore, there are elements—and I have seen it in my previous life—where there will be this constant contesting of disclosure.

While police practices need to improve and we need to apply due diligence, and make sure that we comply with the law, simply now—legislatively, right across policing—disclosure needs to change. If you think that disclosure has now emerged over the last 20 years, we do not have just disclosure on paper but we have disclosure which extends to digital, and there is significant crossover when you look at multiple devices. If I had to do one thing, I would probably look at that.

The second thing—and I have talked about it a lot—is around how we get that data, how we interrogate that data and how we identify the people who are causing the most harm. I know that that is at the forefront for certainly my colleagues right across law enforcement and in the National Economic Crime Centre but also in banking. There are elements there that are the two big things that I would wish to change. If I am limited to two, I will take those two, and Pete may have another one.

Peter O'Doherty: I would say that a significant number, if not the majority, of economic crime cases are enabled by changing technology. In some cases, we are looking for a ghost. We are looking for a machine, a botnet or a DDoS that has committed this offence. It is how you recruit the right people into policing, with the right skills, how you keep them and how you make sure that we can match the pace at which criminals develop these capabilities. It always feels like we are behind and that is really difficult. One of the reasons why some of the cases are not investigated, whether it is a high loss or a low loss, is because the only line of inquiry we have is a website in a jurisdiction that we cannot touch or it is a piece of technology we just do not know how to get round.

What we are doing around that is we are working with a significant range of volunteers, like special constables, who currently work in banks, in risk and compliance, or who are graduates in computer science. These are young people learning around ethical hacking and penetration testing. We even have Microsoft working in our department and looking at those computer service frauds that I spoke about before, thinking, "What can Microsoft do to improve its education to consumers and upgrades to its software in order to engineer out that threat?" It has to be in partnership. It is all about intelligence. It is about somehow staying ahead of the game, but policing culture has to change. It is about finding people with the right skill sets. That might be going to universities and to businesses, building capabilities through volunteers and just becoming much more digitally enabled in the way we work.

Chair: If you were able to solve Microsoft's update for computers, you would have millions of subscribers around the world who would be delighted, so thank you.

Q595 **Mr Baker:** Good morning. Commander, you told us an achievement of the Joint Fraud Taskforce earlier. Could you tell us a little more about what has been achieved since the then Home Secretary, Theresa May, announced the joint taskforce in February 2016?

Karen Baxter: The benefit of the Joint Fraud Taskforce is that it brings various agencies together at the right level. There is a collective move towards this. When we were looking at the Banking Protocol, there were certainly challenges in that. The secret of this is about harnessing the energy to get something like the Banking Protocol rolled out. Quite often, what we find is that the various needs of the various organisations tend not to gel. The Joint Fraud Taskforce has, to some degree, caused us to gel and be more collective around that.

When you are looking at the £40 million that was taken, the average prevention per call in terms of the Banking Protocol was about £7,000, and it is important that we know this. When you extrapolate that across various victims of crime, and the longer-term impact in terms of preventing that, the impact with those individuals is quite important.

At the moment, at the Joint Fraud Taskforce, we have gone through a review and taken stock of where we wish to be. Also, a new chair has just recently been appointed. We are working with them and now looking to see where the thematics are for the next number of years. Through the Joint Fraud Taskforce, we have implemented Take Five to Stop Fraud, which is a campaign encouraging people just to take five minutes. Quite often, as Peter said, if it looks too good and feels too good, it is probably too good. It is about the power of getting people to take five minutes and to take a step back. That in itself will have prevented many crimes. It also opens up the discussion for victims.

A number of other protocols that we have developed are about getting fraud education into schools and about drafting lesson plans. Going back to how policing delivers, some of the fundamental police delivery—the neighbourhood officer—is engaging with frontline individuals, with citizens and with young people in the 11 to 18-year-old bracket. It is important that we can develop those types of packages and materials that we can share with younger people.

Q596 **Mr Baker:** You mentioned the clash of interests at the different organisations involved, which, of course, is inevitable, and the thematic issues. Wycombe being in Thames Valley, the Police and Crime Commissioner, Anthony Stansfeld, has brought the Lloyds/HBOS fraud in Reading to my attention. I wonder if you could tell us what has been achieved amongst these organisations around the allocation and funding of those kinds of investigations. The reason I ask is that it does seem to me that it speaks to this clash of interests because, if I have understood correctly, Thames Valley ended up prosecuting that very complex and burdensome fraud because no one else would, and it was worth hundreds of millions of pounds. I wonder if you could tell us a bit about how the taskforce can make more effective the investigation of these very important and large-scale frauds.

Karen Baxter: You are quite right that there were cases in the past that had moved around various organisations. The whole establishment of the National Economic Crime Centre is designed to design that out, if at all possible. There will always be a clash of agendas and cultures across organisations. What I would like to reassure the panel of is that I see less of that today. I see absolutely less of that today than I saw 15 years ago, and that is really a good, positive thing. I see an absolutely collective will to have discussions, to have multilateral work and to have bilateral work.

For example, yesterday, I met with some of my colleagues in the financial crime authority about how we develop. They have a need and we have a need, so how do we develop that better? We are in an era where those

communications and that collective good will is working much better. The National Economic Crime Centre is working in a way that it is pulling, in a formal, mandated way, those organisations together and one where we start to have more honest and constructive discussions. The National Economic Crime Centre is also about understanding what cases should be at the top end of offending and investigated by certain organisations, and also which of those cases then start to go out to respective organisations.

It is certainly in the early stages at the moment, but what we are really working hard on is trying to get clarity around who investigates and when. The biggest thing about the National Economic Crime Centre is that it is perhaps a lead force with specialist assets from other parts of law enforcement. That is when we start to get a really dynamic approach. We are not there yet. We are in the early stages. That is where we drive to be.

If I could just add one more thing, that does not just stop at the National Economic Crime Centre. That is what we are trying to do as the national lead force. We have had some police transformation funding. We are working with that funding to increase the footprint that we have as the national lead force and how we provide better support to ROCUs and to 43 forces. What was really helpful recently was the HMIC report, which indicated those gaps, and now we understand that and we have had that independent verification, we understand how we need to work better. If there is a case that is in a police service, we understand how to either get the specialist assets to help it investigate or bring it to the appropriate central authority.

Q597 **Mr Baker:** You have been very clear in what you have said. At the moment, that is still something of an open question in terms of who investigates when.

Karen Baxter: I could not give you a list to say ABCD is investigated by DEFG. What I see and what I am really encouraged about is the fact that there are many more discussions now. There is also a concern, if I am being very frank. Every force has a finite amount of resources, people and money. UK policing has a dearth of detectives. We are absent in the numbers we would like. Therefore, every force, every ROCU and the City of London feels that. When there is a case that comes to a particular police force, there is naturally sense of, "Is it ours or who does it belong to?" In terms of a case meeting a certain threshold, if it comes to the City of London, it will have a threshold whereby we would test whether it needs to be investigated by the City of London. Equally, if it goes to a ROCU or if it goes to the National Economic Crime Centre, is it set in absolute stone that it is ABC? I would say that there is some degree of technical data and matrix, but there is also much more of a discussion. We are moving to a much more mature phase of doing business.

Q598 **Mr Baker:** It seems to me to that there is a real problem with both finding the expertise to investigate this kind of fraud and allocating the cost of doing it. The real problem is the victims, of course, because all of

us here will have seen businesses that feel, one way or another, that they have been extremely badly treated by their banks, possibly up to the level of criminality. Of course, they are the ultimate issue, but in terms of helping them, where is the expertise and who is going to fund the case? That was the real problem for Anthony Stansfeld.

I should prefix this by saying you have given us a wonderful insight into the range and scale of your challenges, and you clearly, rightly, take pride in what you are doing, but I hope you will not mind me saying that at the moment I am not sure at all that, if, in the future, it emerged that a large number of businesses were suffering a pattern of what seemed to be criminality around a particular bank branch, a fraud perhaps worth hundreds of millions of pounds would be smoothly allocated to well-funded experts who would bring that successfully to a conclusion. What can the joint taskforce do to concretely deliver clarity about how things like that would be prosecuted?

Karen Baxter: I am interested in the terms "smooth" and "concrete" because I am not sure that smooth concrete is something that we work well with. I do not mean that flippantly and I would love to get to the world of smooth concrete, but we absolutely have recognised that we have looked at that case. For us, it is about understanding the threat. When you have a linked series of incidents, that is where you have to start at the beginning. If you have a national lead force with a national reporting centre, that is designed to try to identify those linked cases. If those linked cases hit certain thresholds, we are really working hard to ensure that they come to the right location. Does it always happen correctly? No, it does not.

When you look back to that case, that probably has generated certain significant discussions around policing. One of those areas is around policing getting its house in order. I am currently working with NECC around the financial crime, and that is about us understanding the threat presented to policing and how we allocate cases and expertise. That is also about how we feed to the NECC, because if we do not have an understanding and clarity about the intelligence of the cases, and the risk and threat that presents, we will not be able to support the NECC appropriately. What would happen is that that would become overwhelmed with 800,000 contacts through Action Fraud.

I cannot give you a definitive that it would be a smooth process from A to Z. What I can give you an assurance of is that it is something that is very much to the fore of how we are working as the national lead force with colleagues across ROCUs. There are a number of pilots that we are working with at the moment to try to pull out how we would task or how we would allocate those particular cases, and, equally as importantly, how, when those cases go out to a force and start to be investigated and it starts to become known that it is a much bigger case, we escalate those through efficiently and in a timely manner to where it needs to go.

I cannot give you what I think you are looking for but I can give you the reassurance that it is absolutely at the forefront of our minds to deal with that.

Mr Baker: I am sure it is something we will have to come back to. I am very conscious of the amount of time I have used but if I can be allowed one more, I am going to try to open up another enormous issue with one question.

Chair: You do not have to ask it in massive detail.

Q599 **Mr Baker:** As I read my brief, I saw that bank chief executives are part of the taskforce. It reminded me that, sometimes, all of us here—and it has been well aired in Parliament—will find that businesses are subjected to behaviour by banks, whether it is the activities of the Global Restructuring Group of RBS or whether it is interest rate swap mis-selling, which reminds me of the old-fashioned parlance of fraud that perhaps a pecuniary advantage has been gained by description, because people have bought products from banks that really they ought not to have bought. They were not sophisticated enough to, for example, understand the interest rate swaps that they were entering into. That then brings me on to derivatives, and it seems to me endemic that derivatives are used to game bank capital adequacy rules. This is, of course, an area of not only the most enormous value but also of profound significance to the stability of the financial system, and it requires an extraordinary level of sophistication to understand what is being done.

Karen Baxter: Sorry, perhaps you could repeat the last bit.

Mr Baker: Yes, of course. I mention derivatives because of the interest rate swap mis-selling, which often strikes me as a kind of fraud, but that leads me on to the other big can of worms, which is derivatives being used by banks to game bank capital adequacy rules and prop up otherwise insolvent banks. The classic example is the Italian bank bail-out but it is done elsewhere endemically.

I wonder, across this range of activities by banks, whether it is something that you feel you should be getting involved with as a taskforce and whether, on something of that enormous scale and complexity, you feel you have anything like the right resources to examine whether fraud is being carried out in those kinds of sophisticated areas.

Karen Baxter: I will come to Pete in a minute with that. The first thing is audit and compliance—another grey person's part of the world. Sorry if anybody is in audit and compliance. It is an absolutely key part of where we start with this. If we have very strong regulation, strong audit and a strong compliance culture, what we do is we deal with those issues at a much earlier stage. We prevent those issues developing and those rogue behaviours getting any degree of traction. That is the first thing.

Do we have enough skills? Pete talked about it. What we do have is we have access, through volunteers and through specials, and we are working to build that even more, particularly with our location in the City

of London. We are working to work not just with individuals but also with the private sector, which is prepared to support individuals who will come into policing and provide that expert experience. That is part of the reason why we rely on our partners. Those individuals will have an expert knowledge that I will never, ever be able to get. Even if I got it, I would never be able to maintain it, because I would need to be exposed to the everyday workings, to the practices, to the judiciary and to all of that to test my knowledge.

For us, that is a complex arrangement that you just discussed there. If we are going to deal with that, we will be ever-reliant on experts coming in from business and assisting us, and we welcome that.

Mr Baker: Could I just close with a point? That has been very helpful evidence but I just would observe that many bank chief executives, as history has proven, will not themselves understand some of these very complex areas of business. Having not understood them, they are not likely to have spotted that it would not be in their interests to solve the problem either. When I see that bank chief executives are involved in the taskforce, that is great because, of course, I am sure they are all decent, honourable people, but history has shown that the kind of business practices that go on are not understood by those managers and, were they to be understood, it would not turn out not to be in their interests to solve them. If I may, I will just leave that as an observation that that is an issue with fraud that I hope, sooner or later, we will tackle.

Chair: We might follow that up with UK Finance. I am not going to go down that road any further because I am going to bring Simon in.

Q600 **Mr Clarke:** It is rather timely because, Commander Baxter, you referred a moment ago to the fact that there is tremendous external expertise that you can leverage in from the private sector, which is something I wanted to talk about in terms of the Dedicated Card and Payment Crime Unit, which has been going for quite a long time now. It was formed as a partnership very much with the private sector and Financial Fraud Action UK. Can I understand the scope of private sector investment in this project?

Karen Baxter: Do you want to start with the scope of it?

Peter O'Doherty: Yes, sure. The Dedicated Card and Payment Crime Unit has been our longest endeavour in terms of a public-private partnership. It is completely funded by UK Finance. In terms of the operational assets we use, it is a mixture of the Metropolitan Police and City of London Police. It very much has a national role in the fight against payment and card crime. There is a lot of expertise around compromised card payments, unauthorised push-payment fraud and banking insiders, which we are seeing increasingly. It has had some fantastic results. A lot of the referrals come from the banking industry into that unit for investigation. They have their own case acceptance criteria around that.

One of our best examples was Project Skynet, which was funded, in addition to the banks, by an EU-funded grant. This was around tackling increasing threats from card-not-present fraud and led to the disruption of multiple numbers of organised crime gangs. We took down 42 gangs, and 27 defendants were charged. It has been in place for well over 16 years now and is only one of the three privately funded units that we have operating from the City.

Q601 **Mr Clarke:** What are the other two, out of interest?

Peter O'Doherty: The second one is the Insurance Fraud Enforcement Department, which is funded by the Association of British Insurers, where effectively insurers pay a membership fee into that. I know the Commander touched on it before but its remit is very much around fake insurance policies, be it holiday or pet insurance policies, but most importantly cash-for-crash. Funnily enough, in the news yesterday, we have charged eight defendants who were operating across the UK, who got 32 years for that offence.

Lastly—we call it a privately funded unit but it is not per se; it is funded by the Intellectual Property Office—there is our Police Intellectual Property Crime Unit, whose remit is very much around counterfeit goods, like high-end fashion goods or automotive car parts that arrive at UK borders like Felixstowe, and the online part of the business around counterfeit music, books, films and software, which again has links to the funding of organised crime.

Those three units have their own accountability mechanisms and performance around them, and are very much held to account on the success they have operationally, but equally the return on the investment value made by industry.

Q602 **Mr Clarke:** Just to understand the quantum of how much money is required to fund the unit, do you have a ballpark figure?

Peter O'Doherty: Each unit invariably has a two-year funded contract. They are different for each unit and I can come on to that now. IFED is our biggest, with over 50 members of staff. The Police Intellectual Property Crime Unit has just over 18 members of staff. The Dedicated Card and Payment Crime Unit has over 20 officers from the City of London Police and the Met. In terms of funding—

Chair: If you do not have the figures, you are very welcome to write to us.

Q603 **Mr Clarke:** It is helpful to understand how significant this is. I suppose the corollary to that is whether it would be possible were that private-sector funding not to exist.

Karen Baxter: Certainly, it is around £2.4 million per annum in terms of DCPCU. I do not have the figures for the other two forces.

Q604 **Chair:** The point that Simon is making is that, given the constraints on

resources, it probably would not be possible to have those units without private sector funding.

Karen Baxter: Yes. We do rely on and we are really appreciative of that funding. It also allows us to share that information. It is an estimated £481 million of savings in terms of reducing fraud for the DCPCU and 800,000 counterfeit and compromised card numbers. Think of 800,000 individual cards and how many people that relates to. We then work with the banks and the banks very quickly then intervene with those individuals to ensure that they are not either a victim or that they eliminate any further offending. It is a really exceptional model and it is one that we hopefully will be looking to develop over the next few years.

Q605 **Mr Clarke:** In many ways, the word "exceptional" certainly points to how we could develop this. If this works so well, are there other examples where you would like to see greater public-private sector co-operation in the space of financial crime?

Karen Baxter: You may have some views about where we might want to take that. Again, on the phase 2, the next iteration of where we need to go in terms of economic crime and getting into that proactive state, there is some fabulous learning around the DCPCU units. We have already commenced those discussions with the likes of UK Finance and with our law enforcement partners around how we can take that concept and grow it. Sometimes it is about growing and piloting that in a more industrialised fashion and that allows us to keep up with the changing and evolving types of crime that we see every day.

Peter O'Doherty: They are very, very much the envy of other countries. This notion that you have a dedicated policing capability that acts for and on behalf of the industry, for demand that otherwise would be unserved by local to national policing, is quite phenomenal, really, and they have a lot of space to operate within. Interestingly, the insurance fraud, the credit fraud and the intellectual property fraud are very much high-volume stuff that traditionally was not reported to Action Fraud and stuff that policing just would not have the priority or capacity to investigate.

If there was one other sector that deserves a bigger service, it is the retail sector, because if you look at online shopping fraud, which is one of the most common frauds reported to Action Fraud by volume and harm, it is very difficult to get the sector the investigative response that perhaps they would expect. I know the industry has been very supportive recently in the last few years around trying to build capability and they are allowed to now bulk-report crimes to Action Fraud. To get them the level of response that they would require we would always welcome some support from that sector.

Q606 **Mr Clarke:** Is that a discussion that you might take forward, do you think?

Peter O'Doherty: It is a discussion that we have had in the last few years, but clearly those industries have their own financial pressures as well. All we can do is provide a clear business case around what the return on that investment would be by way of outcomes, the prevention of harm and protecting consumers, but it is very much for the industry to decide if that is an investment they want to make.

Q607 **Mr Clarke:** It is, except insofar as there is obviously a public interest in making sure those crimes are addressed, is there not? This slightly leads to a question about whether there are any risks in accepting private sector resourcing in this way, because it does mean that both where that funding continues and indeed potentially to a degree how it is focused is contingent on non-state priorities. Is that a concern in any way?

Karen Baxter: You hit on a really good point. I am sure Peter will come in here. One of the things is about always understanding where that line is. People might say it is cash for hire. We do not see it like that and there is sufficient challenge within the construct of how we work with our partners to ensure that that is not the case. We try to work more with the associations and a representative body, so that puts some distance from that potentially happening.

Where we see this is that they grow very strong models of investigation. Those models are recognised right across other jurisdictions, for example in America, around the innovation and because they are working collectively very close together—DCPCU is working with bank investigators—there is a much quicker evolution in how we understand that type of offending. That is where we can really start to grow this business in a more industrialised way for economic crime.

Q608 **Mr Clarke:** I can see that it gives you access to a range of expertise that simply could not feasibly otherwise be generated. I have a final question. In terms of the challenges that these units have faced, how have you worked to overcome those and what have been the biggest ones in terms of this unusual working relationship with the private sector?

Peter O'Doherty: I know this perhaps is not what you would expect, but there have not actually been that many challenges. The biggest one for me is around the reporting performance, and there are two parts to this. When you think about policing and you imagine what a police officer does, you think about arresting people, and the industry want people locked up and they get that. Equally, some of the work the funded units do is not just around locking people up; it is around understanding the harm and working with the industry to protect consumers, to help design policies and practices that protect consumers and protect the industry. That was an interesting dynamic, first of all.

Q609 **Mr Clarke:** That is the wider dynamic with the public though, is it not? The public would always want to see certain forms of accountability.

Peter O'Doherty: Definitely. Equally, if you think about austerity measures and that policing across the country has lost up to 30% of its

operating budget, but then you save the 10% via the increase in precept locally via council tax, we can show quite clearly that without that funding those roles would not exist. The challenge has been us culturally changing our entrepreneurial ability to show that clear return on investment. It is not just about, "If you pay for 10 police officers, we will lock up 50 people". For example, £481 million in savings has been achieved since the inauguration of the unit. When you compare that against the investment, there is a clear return and value for that industry. It has required police to become more entrepreneurial and executive in our approach, which we have absolutely welcomed.

We get brilliant support from the unit and when you look at other policing teams, where you look at reducing overtime headcount, these units, because they are funded privately and they have a clear national focus, are more healthy in that respect, because they have that dedicated funding line. It is quite an interesting dynamic.

Mr Clarke: It is fascinating and encouraging. Thank you both very much.

Q610 **Rushanara Ali:** I have a few follow-up questions. Earlier on you mentioned that there is a need for greater transparency from the banks, following up from Wes's point. I just wondered if you thought that it would be sensible for the banks to be required to make the reports, either in aggregate of the number of fraud issues that have come up to the police or individually when those reports are not coming to you directly from the consumer. Who would like to start?

Karen Baxter: When we look at the volume that we are facing, the banks are also dealing with that volume. I am probably not going to prescribe what the banks should do. There is a construct certainly at the moment when we look at SARs. SARs is currently under reform and rightly so. We are involved in that and it is around understanding what those reports should look like and how meaningful they can be. Are we looking at volume or are we looking at the key issues? You could say, "We want absolutely everything completely and utterly transparent and it is there", but does the bureaucracy beneath that make it a system that does not work?

Q611 **Rushanara Ali:** Just to get some clarity on what is going on in the system, without relying on your limited resources or the public coming forward, is there not a responsibility on the banks to invest in the technology to be able to tell us? They monitor this stuff in terms of how many people are ringing in or alerting the banks of the number of fraud reports that they are having to make. Should that not be a requirement?

I will give you a parallel, and it is linked to the last point you made, DCS Peter O'Doherty. Is that correct? People often fail to pronounce my first name correctly, so I feel for you. The parallel would be with Facebook and other online activity, for instance counterterrorism activity, where the requirement to force them to take things down before the police have to individually take them down is a positive development. It took some

years before this happened. Should we not be learning from those examples, so that proactively those companies take the lead in reducing the need for you to have to collate the data in the way that you are doing, which is not comprehensive at the moment?

It is really to help you build a picture. It seems to me from everything we have heard this morning that there is an inadequate picture, in part because the banks are not taking that responsibility. If they invested a fraction of the money that the public are losing from banking fraud, then perhaps some of this could be prevented. Perhaps it is not happening fast enough. This inquiry will have the opportunity to make recommendations. My question is whether this should be one of them—yes or no?

Karen Baxter: I am not going to give a yes or no, because that would be very limited. The first thing is, in terms of the banks, they have an absolute responsibility, and I agree transparency is essential. As far as possible, they should be providing us with the information that we require. How they do that is a matter for the banks. They need to work that out, and they need to work out not just how they do it but the extent of the issue at the moment. I am not sure we all understand the extent of the issue.

Q612 **Rushanara Ali:** With respect, it is a matter for Parliament and the regulators of the banks to get this right, so that our constituents do not become victims of fraud.

Karen Baxter: Absolutely.

Q613 **Rushanara Ali:** We have seen the evidence. You do tireless work, but it is not about what you do; it is about a systemic failure still in the banking system. With technology failures, like the Lloyds TSB example that we saw, with nearly 100,000 complaints, more of this is going to happen, so we need the banks to step up. We do have the opportunity to make recommendations to the FCA on what they should do to ensure that the banking sector, perhaps more with proportionality built in, can provide the evidence to you, either in aggregate or not, depending on whether it is appropriate to do that.

Karen Baxter: We would absolutely welcome that evidence being brought from the banks to us. Also, what we would encourage is that there are elements of analysis and understanding around that information, because I go back to the point that I am not sure we need any more millions of bits and entities of data. What we need is to understand what the data is saying for that sector.

Just to finalise, that is one part of it and the other part of it is that it is about a whole-system approach, and that is around the SARs reform, which is essential at the moment in terms of how we all respectively take that information, wash it across and understand where we are.

Q614 **Rushanara Ali:** Earlier on, throughout the evidence session, you talked about the need for co-ordination and joined-up working, and many of the

positives that are there. Forgive me if I have not fully understood this, but what is not entirely clear is how an investigation happens and joined-up working happens. If, for instance, you have a crime that is perpetrated in one area of one police force and the victim lives in another, how does that work? Do you feel that there are sufficient arrangements to ensure there is joined-up working with investigations? I can see that the collation of data is much more advanced in your work.

Peter O'Doherty: Yes. Normally we will have a network of crimes, and there are five criteria in priority order that we go through to determine where that network of crime goes for investigation, because it is quite rare to have one crime in Manchester that goes to GMP. You invariably have an offender and three victims in three force areas. You have five steps to work out where the crime should go for investigation.

What happens at the moment is if the local police force that we decide is the owner of that investigation thinks it is a bit complex and it should be a regional response, they can then push that up to the ROCU for investigation, but it has limited capability. Where it is a multiregional response, which was a case mentioned before, that will then come through to the national lead force, and we have the capability to investigate that nationally.

To answer your question, the five steps work really well, but what can be improved, which is something the NECC will achieve going forward, is that ability to step in, intervene and make a decision around whether a case should be owned nationally, regionally or locally. Until we achieve the levels of capacity we require, there are always going to be some issues around ownership of the cases.

Q615 **Rushanara Ali:** That takes me neatly on to capacity and resources. Given that the level of violent crime has doubled in the last three years and given the other pressures on the police service—a reduction of 21,000 officers and in London we have had hundreds of millions of cuts and another £400 million to go—why should the public have confidence about this particular form of crime? You have said yourself, and we know in our constituencies, that people are very concerned about knife crime and violent crime. The police have the impossible task of trying to balance and make those choices about priorities. What would help in terms of additional resourcing in order to address this problem, which is not going to go away? In fact, it is likely to grow. What should this Committee be recommending to the Government?

Karen Baxter: One of the first things is that over half of all economic crime is linked to cyber or fraud. When you look at that, can we honestly say that over half of all the money that is used in this country around victim support and how we support victims goes to the victims of fraud and cyber? That is one of the areas that we certainly are looking to develop with PCCs, around how they, along with local chief constables, apportion perhaps parts of the local budget and parts of that local

resource around fraud, economic crime and, to some degree, cyber. That is one of the first things that we should consider

Q616 **Rushanara Ali:** What is the budget allocation at the moment in this sphere?

Peter O'Doherty: Do you mean in terms of victim support for that?

Rushanara Ali: Just overall, what are we spending as a country on economic crime, to prevent economic crime and tackle it? What is your budget?

Karen Baxter: I would not have that figure right at this stage. We can write back and provide that at a later stage.

Q617 **Rushanara Ali:** Should you have double the budget or triple the budget? That is the question. Perhaps you could write to us to say what would enable you to achieve the objectives you are trying to achieve and the scale of the problem as it grows. What is needed? Otherwise, there is a real danger that this just gets worse. You are running to keep up and, in fact, given the pressures, we are not going to achieve what we need to achieve in this arena.

Karen Baxter: Can I just say one thing about funding? I will be brief. While we are grateful for the likes of this transformational funding and we are using that as best as we can to build capacity and capability, one of the challenges is the short-termism, so the 12 months. We find it incredibly difficult in 12 months to be able to recruit people, vet people, bring them into the system and then professionalise those people in a way that really adds difference. We have had this discussion this morning. In terms of real, meaningful change, we are looking at a three-year business cycle by the time that we come in, we get that funding, we get those people, we test them and we continue to evolve. That, for us, is one of the key things that this panel could make recommendations around, if that is within your gift.

Chair: The long-term funding.

Karen Baxter: Yes, the longer-term funding. We accept due diligence and due accountability. In fact, we would embrace that.

Q618 **Rushanara Ali:** I just had one final question, which is related to the Credit Suisse case led by the US, with the arrests of London-based bankers. It is a $2 billion fraud case that was reported last week. I do not know if it is a City of London Police lead or an NCA lead, and then there is the FCA dimension. In a Reuters story, Tim Jones, a policy officer at Jubilee Debt Campaign, said that it was the London branch of Credit Suisse and VTB that lent $2 billion, yet there has been a shocking lack of action taken by UK authorities in holding them to account. Britain's financial watchdog, the FCA, started looking at Credit Suisse in 2016. The FCA declined to comment on latest events.

Despite the financial crisis, this happened recently and it is an example of

where things are still going wrong and we are relying on the US to take action before things get dealt with in the UK. Do you think a case like that exposes the fact that we still have a long way to go, both in terms of resourcing units like yours—the NCA and others—and in terms of what the FCA can do? Are we still pretty impotent in dealing with these cases compared to the US? You mentioned something earlier about the US.

Karen Baxter: First of all, I am not entirely aware of the case and I will not make comment per se on that case. Mistakes will always happen.

Q619 **Rushanara Ali:** That is a very expensive mistake at $2 billion.

Karen Baxter: I do not know the details well enough to explain or to defend or whatever, but mistakes only happen when police officers do nothing, sit on the fence, do not exercise the legislation that they have been granted and do not audaciously use all of the things and the assets that we have been provided with.

Rushanara Ali: When officers do not.

Karen Baxter: When officers or when anybody in law enforcement is given that—

Q620 **Rushanara Ali:** It is your profession, but is it not a tall order at the moment, given how much pressure our officers are under? I see it and my colleagues will see the amount of pressure police officers face in their constituencies. I do not need to tell you this, because you have lived through it. You live and breathe it. It is really difficult to be proactive and to be able to cover all the bases, particularly in this area when it is not as immediate as violent crime and the other challenges that the police are dealing with.

Karen Baxter: Yes, and that is exactly the reason why, when we do make mistakes, we need to collectively learn from those mistakes. It is not just about policing learning from those mistakes; it is about all law enforcement. When you look at the National Economic Crime Centre, what that does is it gives us collectively, across law enforcement, the opportunities to learn from those mistakes, and that is absolutely critical in improving our stance going forward.

In terms of the US, they have a very different system in terms of judiciary. They have a very different system when it comes to sentencing incentivisation. In terms of having people who are criminals, who, to use the term, we turn, and then we have them work and provide us with evidence, that is much more the culture in the United States than it is here in the United Kingdom.

The third thing is in the City of London we have a secondment in the District Attorney's Office in New York, and what we see is that that is critical around UK policing being embedded in some key jurisdictions elsewhere in the United Kingdom. Are we impotent? No, we are not

impotent. I would say that is much too strong a word and one that I would walk away from.

Q621 **Rushanara Ali:** What word would you use to describe us relative to the US?

Karen Baxter: I would say that we are in a reasonably good position; we know where we need to go and what we need to do. We have a resilience in UK policing that perhaps does not exist in any other form of policing across the globe. I certainly have not seen that. What I do see at the moment, and I have already alluded to this, is that there is a willingness and a collaboration across law enforcement that reassures me like it has never reassured me in the last 15 years of my policing.

Does that mean that it is going to be easy? No, it is not going to be easy. In fact, I would say I probably have some of my hardest times in policing in the next 18 to 24 months, but what I do have is an absolute hunger to take it forward, not just for the City of London but also for the National Economic Crime Centre.

Q622 **Rushanara Ali:** Why the next 18 to 24 months?

Karen Baxter: When you look at NECC and when you look at the collective will of people across agencies, there is an absolute desire by people in leadership roles and right throughout those organisations to try to address those issues. That is not going to be done in isolation of law enforcement. It is going to be done because of forums like this, because of accountability, because of legislation changing when it needs to change, because we have identified it, we have been testing it and we are taking that forward. I welcome these types of forums, because it is through these that we hopefully will take it forward, not just as law enforcement, but as a nation.

Chair: Thank you very much. That has been a fascinating session and I am very grateful to you both for your time and evidence this morning. We will continue with the inquiry. We have taken on board the points you have made and the suggestions you made for recommendations. Thank you very much for your time and best of luck with all your work. Thank you.