HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Policing for the future, HC 515

Tuesday 9 January 2018

Ordered by the House of Commons to be published on 9 January 2018.

Watch the meeting

Members present: Yvette Cooper (Chair); Rehman Chishti; Sir Christopher Chope; Stephen Doughty; Preet Kaur Gill; Sarah Jones; Tim Loughton; Stuart C. McDonald; Will Quince; Douglas Ross; Naz Shah.

Questions 243–310

Witnesses

I: T/Commander David Clark, National Co-ordinator for Economic Crime, City of London Police, Richard Piggin, Campaign Manager, Which?, Detective Superintendent Nicky Porter, Financial Investigations Unit, Serious Crime Division, Greater Manchester Police, and Katy Worobec, Managing Director, Economic Crime, UK Finance.

Examination of Witnesses

Witnesses: T/Commander David Clark, Richard Piggin, Detective Superintendent Nicky Porter and Katy Worobec.

Q243 **Chair:** I welcome the witnesses to our evidence session this afternoon, which is part of our ongoing inquiry into policing for the future. Would each of you begin by introducing yourself, saying where you are from and telling us, very briefly, what you see as being the main trends in online fraud that you are facing?

Katy Worobec: Good afternoon. I am Katy Worobec. I am Managing Director, Economic Crime, at UK Finance. We are a trade association of about 300 banks and other financial organisations. It is made up of six existing trade associations that merged in July last year, one of them being Financial Fraud Action UK of which I was director. I have been working in fraud for a good number of years now.

We have a fairly narrow view of online fraud, so I will tell you about what we consider to be in the bucket called online fraud. The first is remote banking fraud and for the first six months of 2017 we saw that reaching just over £73 million. That was up 3% for the same period in the previous year. The other aspect is "card not present" fraud, which is fraud made on purchases over the internet or by phone, and that totalled £205 million in the first six months of 2017. That was slightly down by 1% on the previous year. Those are the key things that we are seeing.

The other aspect is the types of scams where, unlike the types I have just described that are unauthorised types of fraud, customers are duped into making purchases or authorising transactions, payments from one account to another. That is an increasing issue that we are seeing and we started reporting on those for the first time in the second half of last year. That was about £100 million of what we are calling authorised push payment fraud scams for the first half of the year. Those are the key areas where we are seeing the trends at the moment.

Detective Superintendent Porter: I am responsible for the Economic Crime Unit in Greater Manchester. The trends are very similar for us. One of the key areas that we are looking at in Manchester is understanding the demand that we take from the NFIB and Action Fraud and what it looks like locally. We are working at the moment to understand vulnerability and prioritising our resources for vulnerable victims of fraud. Since we have started this new modelling we have seen that over-65s are being contacted more online and by telephone as well as the traditional type of bogus trader offences with that cohort of individuals. It is very much a similar position; card fraud online is the biggest demand for us in Manchester.

Richard Piggin: Good afternoon. My name is Richard Piggin. I am a Campaign Manager at Which?. We are the largest consumer organisation in the UK and as such we regularly hear stories from consumers about

their experiences of online fraud. We have also investigated different types of online fraud from holiday accommodation fraud to the different frauds that consumers face when using social media sites, for example. With "card not present" fraud, the detriment, the impact on consumers is often relatively little in that often they receive all their money back.

The area we have been concerned by is the increase in bank transfer fraud or, as Katy has referenced, the authorised push payment fraud. In those circumstances, at the moment the consumer has no legal right to get their money back from the bank and often is left significantly out of pocket. We raised a super-complaint with the Payment Systems Regulator in 2016 on this issue and as we issued that super-complaint we heard from over 600 consumers who said that between them they or someone they knew had lost a total of about £5.5 million.

Those figures are then backed up, as Katy said, by the UK Finance figures at the end of last year. In the first half of 2017 over £100 million was lost to this type of scam. Only about 25% of that was returned. The average consumer loss was over £3,000, so we are talking about life-changing amounts of money. That is why we focus particularly on that type of fraud and perhaps later we will talk about some of the efforts that are being made to address that.

T/Commander Clark: Good afternoon. I am David Clark, Commander for the National Lead Force, City of London Police, which takes responsibility for co-ordinating the fraud response across policing in the UK.

The national fraud and cyber-crime reporting centre, Action Fraud, has seen a 37% increase in reported fraud and cyber-crime over the last three years. That is significant. There are many figures floating around on volume and value in categorising that. I try to stay away from volume and value and talk about impact and harm. This is about the victim; that is where I come from. In respect of loss and volume, it depends which one you refer to as to what fraud type is the most worrying or the biggest trend over the last 12 months, for example, but I will go through two or three to help.

Cheque, plastic card and online bank account fraud remains a high priority and a high volume and significant loss in online fraud. Online shopping fraud and auction fraud has risen and continues to rise, and I think that is significant in the way that we lead our social lives now by shopping online. Computer software service fraud, where you are cold called and told that there is something wrong with your computer and taken through steps that effectively disable your computer, has risen significantly over the last two years until a sharp decrease in June 2017 when the national fraud reporting centre were able, by economy of scale, piece together the individual 2,500 reports per month that were coming in at that time and identify UK-based offenders and arrest them. That has led to further action upstream overseas, in particular in India, working

with our National Crime Agency colleagues to address the upstream problem, which is where the call centres were operating from.

Finally, I would mention the recent rise in HMRC tax demand fraud, which is perpetrated through social media, generally by either e-mail or telephone text messages. We have seen a significant rise where the payment method demand from fraudsters has changed from using bank accounts and bank cards to payment through iTunes vouchers and those payments are making their way to China. We have an intelligence gap in that respect at the moment but it is one that we are rapidly trying to fill to get to the bottom of why and the methodology that is being used.

Worryingly, 33% of the methodology used by the fraudster in the trends that I have just identified still comes over the telephone. In a third of all reports that come to us, the victim says that the contact initially was made by cold call telephone, online sales is 15% and the next biggest would be e-mail contact at 12%.

Q244 **Chair:** We have a range of questions about all sorts of different issues, so don't answer questions if it is not relevant to your area of knowledge and expertise. What is your sense of the pattern of who the offenders and criminals are and where they are based?

T/Commander Clark: A huge amount of analysis goes into this. The 600,000 reports that come into the Action Fraud centre per year give a great opportunity to see the demographics of the offenders, not just where they are based but where the funds from fraud go to. The most common destinations are the US and within Europe. That is the first landing point of the offender-based location and the first landing point of where the money moves to. Of course, they move on from there as well.

Q245 **Chair:** When you say Europe, do you mean non-UK or do you mean Europe including the UK?

T/Commander Clark: Including the UK in a local more opportunist fraud sense and outside of the UK when it comes to organised criminality. There were 1,400[1] reports this year of organised criminality where the offender was cited as being based EU-wide outside of the UK[2]. At present we would say there are over 1,100 organised crime groups operating across the economic crime sphere. That is not to say that they just operate within economic crime but they do fraud among their other criminality as well. In the rising trend of software service fraud, which I mentioned in my first answer, it is undoubtedly the case that the call centres led back to it being based in India. That is why we are working with the Indian authorities to take upstream action there.

I can show a complete contrast if I talk about investment fraud and boiler room fraud, as it is commonly termed. In that case, we have worked with

[1] **Correction by witness:** This figure was misquoted; the correct figure is 14,000 and is corrected in response to Q261

[2] **Correction by witness:** This figure is also inclusive of non-EU jurisdictions.

our Spanish national police colleagues and often find that it is UK individuals domiciled in Spain who have been perpetrating the fraud. They are the younger, organised elements of organised crime groups and, as I said, in India organised crime groups are perpetrating fraud through call centres. It varies depending on the fraud type that you talk about and the location of the offending.

Q246 **Sir Christopher Chope:** Can I ask Commander Clark about the way in which Action Fraud works? You just said that you are receiving an enormous volume of reports—600,000 a year. How many of those are you able to investigate?

T/Commander Clark: The first thing to clarify is that Action Fraud does not investigate anything. Action Fraud is simply a call centre and an online reporting facility for victims of fraud and financially motivated cyber-crime. The call centre on the online reporting tool is a repository that sends all of those reports to the National Fraud Intelligence Bureau. That is where the analysis takes place and the economy of scale is brought to piecing together the commonality of all those reports.

Of the 600,000 in 2016-17, 280,000 were categorised as Home Office crimes, in other words crimes that can be counted under Home Office counting rules. That is less than half of all reports, but the other reports are not to be dismissed because although they do not count as a crime on official statistics, there is often action that can be taken against them, such as disruption, or they add to the intelligence picture of the crimes. I would suggest that half of those 280,000, if not slightly more than half, are deemed under a case assessment matrix as viable for inquiry. That means that they will be sent out to UK police forces and beyond for action and investigation. Out of the 280,000, actually my figures would suggest—and I apologise—that 25% went out in 2017 for investigation purposes.

In respect to outcomes from that, fraud has a long tail and so you do not and cannot compare figures within a 12-month period. You would struggle to compare figures for fraud over a three-year period by the time the investigation is pursued, the case comes to court, the trial occurs and eventually you do or do not get a judicial outcome. If I took it on a yearly basis—but I would suggest that is unreliable—there was an outcome for 14% of what went out for investigation last year, if that helps.

Q247 **Sir Christopher Chope:** Is the case assessment matrix that you use a public document?

T/Commander Clark: I don't think so, but I can check and write to the Committee on that.

Sir Christopher Chope: I think it would be quite useful to see it.

T/Commander Clark: There are certainly no secrets in there and I am trying to calculate in my head why I would not make it available to

people. I cannot see any reason, because there are no secrets in there. It is based on the management of risk in law enforcement, a MoRiLE assessment. It is managed on the basis of whether there is an offender that it is viable to put police resources against, that is you are not chasing ghosts. It is often based, depending on the calibration, on the significance or impact of the loss and the harm on the victim. There are many criteria that are assessed along the way.

Q248 **Sir Christopher Chope:** My concern is that there are a lot of individual cases, nitty-gritty cases, often not involving cyber-crime or online fraud, which are being referred direct to your organisation by local police forces. As soon as you phone your local police force, the first point of call, they say, "Refer it to Action Fraud". The constituent or the victim is then under the impression that it is going to be investigated and, as you have just said, it does not mean it is going to be investigated at all. Bearing in mind that maybe 40% of these fraud cases are not cyber-related, would it not be better for those to be investigated at the first instance by local police forces? I have a lot of examples in my constituency, and I will not bore you with them now, of individuals who defrauded other individuals in a criminal way. It is plain as a pikestaff that there is a criminal case with a strong chance of getting a conviction but the individual police forces seem to give the sort of slopey-shoulder response, "We passed it to Action Fraud" and then the victim thinks that it is being investigated when it may well not be.

T/Commander Clark: I can understand exactly what you are saying. This is what makes this new criminality of online fraud really complex. It is complex to understand for the victim, policing and citizens of the UK. The reality is that if the individual goes to their home police station and makes a report of fraud, the local police can make a decision, as if Action Fraud did not exist, on ownership of that crime. You have the offender, victim and location triangle and it is very different for online fraud. The victim may live in Greater Manchester, for example, and they have been defrauded in their home in Greater Manchester. The reality is that the bank account may be outside the jurisdiction of Greater Manchester police and the offender could be somewhere completely different in a different jurisdiction to Greater Manchester police.

The national system has developed where the best place for investigation is the offender location, not necessarily the victim location. In traditional crime it would be the victim location, so if it was an assault we know who the perpetrator is, who the victim is and the location. That is very different in online fraud and the best chance of pursuing an investigation is to give it to the organisation or law enforcement agency where the offender is based, because that is where the collar will be felt.

I understand that that can be very frustrating for the victim. We have done a huge amount of work, and there is more to do at local level and national reporting level on the management of that expectation, but it is

a very complex area. I understand that the victim might not see that and I fully get that.

Q249 **Sir Christopher Chope:** I can understand your response, particularly in relation to online fraud, but my question was also directed to ordinary fraud, non-online fraud. Is there any need for this great centralised bureaucracy for cases of non-online fraud? In my experience, that bureaucracy is being used to deny victims of fraud getting a proper investigation of that fraud from their local police forces.

T/Commander Clark: I will try to be really clear, and I am sorry if I was not clear. There is nothing to stop a local police force taking ownership of and responsibility for a crime where the offender, the victim and the location are in its force area. All they need to do is record it centrally, so that there is a central recording of the facts and the intelligence, and get on with the job.

Q250 **Sir Christopher Chope:** Is that what most local police forces are doing in practice?

T/Commander Clark: I am not aware if they are or not but those are the facts.

Q251 **Sir Christopher Chope:** Are you encouraging them to do just that?

T/Commander Clark: Yes, absolutely.

Q252 **Sir Christopher Chope:** One of my constituents made a complaint, got a reference number and received a letter from Action Fraud saying, "Sorry you have been a victim of crime. All Action Fraud reports are passed to the National Fraud Intelligence Bureau and we review every crime to identify investigative leads as opportunities to disrupt criminal activity. We have reviewed your report and I regret to inform you that we have not identified any leads that will result in a successful criminal investigation." That is from the National Fraud Intelligence Bureau to which Action Fraud referred the matter, but Action Fraud themselves had earlier written to this constituent saying, "The NFIB review the information you have given us and assess whether there is enough evidence for the police or appropriate law enforcement organisations, such as Trading Standards, to investigate your fraud", which is a completely different test. The impression is given in the initial letter to the victim that the fraud is under investigation but the subsequent letter makes it clear that because of the matrix to which you refer it is not. What could be done to make the ordinary victim more conscious of the need to put pressure in the first instance on the local police to take a grip on it?

T/Commander Clark: After this session, I would be interested to see the dates on the letters to see whether they are the current letters that are sent.

Sir Christopher Chope: These are December 2016 and January 2017,

just to answer that question.

T/Commander Clark: It may be that that has changed, but certainly better wording would be advantageous, from what you have pointed out to me. It still remains the case that Action Fraud takes the report and, as it quite rightly says in the letter, it passes it to the National Fraud Intelligence Bureau for assessment. It is not an investigative bureau; there is no investigation. It is an assessment for investigation and if there are viable lines for investigation it is sent out for investigation, whether through policing or another law enforcement agency at home or overseas.

A new way of having to think with this type of criminality is that pursuit is not always the best option. For example, on 170,000 cases in 2017 disruption was seen as the best form of action over investigation for all kinds of difficulties. What I mean by disruption is that if there is a crime that is not viable for investigation, central disruption by removal of website, seizure of money in a bank account, disablement of telephone lines, takes place as well. Unfortunately Home Office counting rules do not record those outcomes but we are working with the Home Office to make that change. It cannot be that we take 170,000 efforts of disrupting fraud and save over £400 million of future fraud by doing that and it is not recorded anywhere, so we are seeking to change that.

Q253 **Chair:** Do any of the other witnesses want to comment on any of those questions?

Detective Superintendent Porter: It might help to give you the context of what that looks like from the receiving end, from Manchester, for Action Fraud. It is a very challenging picture and demand for police locally. In Manchester we have approximately 500 to 600 crimes a month where the offender and victim are in Greater Manchester, so they would be local offences for us to investigate. In addition to that, we have about 800 to 1,000 victims in Manchester who have been defrauded and the offender could be anywhere in the world. It is trying to make some sense of that and it is important that, in my opinion, we have Action Fraud to disseminate the bigger picture because we are going to have victims in Manchester coming to us to report something online or a phone number and it might feature in a wider context elsewhere. It does assist us but it is a challenge.

Q254 **Chair:** If I have got those figures right, you are saying roughly a third of the cases that you deal with have local offenders and two-thirds are somewhere else?

Detective Superintendent Porter: Yes, and it is about assessing who those victims are, are they vulnerable, what services do we need to give to them in Manchester. They are residents of Manchester, however the offender may be elsewhere.

Q255 **Tim Loughton:** I have a constituent who received an almost identical letter to the one Christopher Chope has, and more recently, certainly the

first one we looked at that basically said, "We can't take any further action". I was not aware of Action Fraud when that constituent came to me and this was quite a big fraud. This was somebody who paid £350,000 for a sportscar that did not materialise. I entirely understand that fraud has become the fastest growing crime and is taking up an awful lot of police time and that a lot of lower level copycat fraud cannot justify a full investigation. I entirely buy that, in the same way these days that if traffic accidents are minor you just need a police report for insurance cover without going through all the parameters. This case of mine, and I have no reason to think it was unique, was a large amount of money, somebody who was contacted personally by somebody who was based in this country and the money was paid into a UK account.

You can ask why on earth did he do it, but that is another matter. The fact is that somebody defrauded £350,000 out of somebody who came to complain to me. The police passed it on to Action Fraud and he received a letter saying, "There is no further action we can take". That slightly goes counter to your advice, Commander, that the local force should have taken ownership of that and it should have been looked at in more detail. It was unique, there was an identified crime potentially and it went through UK finances. I might come on to a comment from Katy Worobec. Where was the fault there? What has happened subsequently is that because I complained the police did take it up, they found the perpetrator who was in jail. They think it is the same person and they are trying to make a case against him. What went wrong there and is that unusual?

The question for Ms Worobec is that in my view there was a fault by the bank there because you could identify the bank account that the money was paid into. Surely that bank should have gone through money laundering processes to identify the person behind the bank account but that account was cleared out immediately it was realised that the fraud had been committed and the identity of the person who benefited from that bank account was not available. It strikes me that was a banking fraud and under bank regulation it has not provided the service it should have done, so there is some culpability there. Who should have done things differently between the police and the banks?

T/Commander Clark: It seems to me that that is highly unusual, certainly the amount of the loss. The elements of the case acceptance matrix and criteria would have flagged up the amount of the loss for investigation. I do not know the full details of the case and I would like to know those to identify the point where clearly it has gone wrong for that victim receiving a service from policing or another agency. It is not for me to surmise now what went wrong because I do not know the full details of the case but it is certainly one on which I would urge a conversation after this Committee to ascertain where the fault was, if there was a fault. I do not know whether it is in the detail of the report, in the assessment criteria and where the offender was or where the money went to. I do not know but I would like to find out.

Tim Loughton: Perhaps we can have a conversation offline.

T/Commander Clark: Absolutely. I would welcome that. Thank you.

Q256 **Tim Loughton:** The financial institution was the recipient of the money, albeit rather temporary in this case. What could it have done differently and is there a liability there?

Katy Worobec: It is difficult without knowing all the facts of the case. The bank will have opened the bank account and received the money following all the KYC regulations that it has to follow. That is policed by the FCA, so all our banks do that and it will have done that. The issue is possibly that the bank account has been used as a money mule account and it has been taken over by a fraudster. What happens is that a fraudster will take control of a bank account once it has been opened. It is not necessarily the bank's failure in not doing the KYC checks at the outset that is the fault. It could be that the fraudster has taken over the account subsequently and then used it. As you say, the money goes into the account and is taken out very quickly. It is often split up and moved into other accounts and out of the country very swiftly, so it is quite difficult to follow the money once it has left the initial bank account.

Q257 **Tim Loughton:** That is interesting and I do not know what the particular details were in this case. If that money had gone into a legitimately set up bank account because of the actions of that person, not somebody who hijacked and used it as a mule, the bank would have a liability, would it not, in being able to identify the person who operated the bank account?

Katy Worobec: If there was any suspicion of activity it would have to submit a suspicious activity report to the National Crime Agency. If it had any suspicion at all that the person operating the account or the transaction was involved with money laundering of any type it would have to report that to the National Crime Agency.

Q258 **Tim Loughton:** It has an automatic reporting responsibility on that basis?

Katy Worobec: If it has reasons to be suspicious that an account is being used in that way.

Q259 **Tim Loughton:** Is using it as a mule by somebody hijacking an account a common way of facilitating such a fraud rather than a legitimate bank account?

Katy Worobec: It is certainly something that we are very familiar with, yes.

Q260 **Douglas Ross:** Going back to the Chair's first question about where the perpetrators are when they commit these crimes, what percentage, roughly, of all online crime is based in the UK and the rest of the world?

T/Commander Clark: That is a really hard one.

Douglas Ross: The Economic Crime Commander for the City of London

Police, Chris Greany, said that 50% of frauds against people in the UK were being committed abroad, and that was in 2016. Is it roughly about 50%; has it gone up; has it gone down? I don't know Chris Greany personally but he was able to say it was about 50% in 2016.

T/Commander Clark: It depends where you make that assessment, if I am absolutely honest with you. On initial reporting where offender-based location is known, in 2017 I can account for 1,400 individual reports where the offender on first point of reporting was identified as being outside of the UK.

Q261 **Douglas Ross:** That is 1,400 out of how many?

T/Commander Clark: 260,000 crime reports. That is on first reporting. Sorry, 14,000, which still is not a significant amount in respect to 260,000 crime reports. Having said that, one offender can be responsible for multiple crime reports.

I think that changes when you start to follow the money and you get a very complex web. Let me give you an example of computer software service fraud. Five key offenders were identified in the UK as the first point of offender based on initial reporting. Every single one of those offenders, when arrested, was representing offenders overseas based in India. Initial reporting would suggest that the offenders were in the UK, but following that though and following the money and the organised criminal gang in its bigger sense takes you outside the UK.

Another example would be banking fraud and Katy Worobec's teams have a sponsored service agreement to fund the national banking team, the Dedicated Cheque and Plastic Card Unit, the DCPCU. I would suggest a large proportion of, for example, ATM crime is by perpetrators who operate within the UK but are from eastern Europe. You have to deal with that complexity of not just where the offender is based but their nationality and the intrinsic lead to others in their organised crime group.

Q262 **Douglas Ross:** I was looking at where they are based. If 14,000 out of 260,000 are outwith the UK—you mentioned the main areas are the US and the rest of Europe—what continuing challenges do you face or are you making improvements in working with these countries to get a resolution?

T/Commander Clark: We make very good progress with the US and Europe. I can give you specific examples. Within the EU we have certain arrangements, such as European arrest warrants, which are absolutely critical and essential to our work in this field. We have the ability, through Eurojust, to form joint investigation teams and we have had a number of successes through joint investigation teams in lots of different areas. A great example would be working with Spanish police partners on boiler room fraud. Another example would be an EU-funded programme for the Dedicated Cheque and Plastic Card Unit over a three-year period that made a significant dent in Romanian ATM fraud in the UK. That was working and sharing intelligence cross-jurisdiction with Romanian police

and UK police as one team. There are significant benefits of working within Europe and the arrangements that we have within Europe currently.

We have significant ability to share with the US. We have cross-jurisdictional secondments. For example, I have members of the Economic Crime Command in the City of London Police who are placed with the attorney's office in lower Manhattan and likewise the Manhattan attorney's office has somebody placed in the City of London Police. We can work very effectively where the nexus is between the two countries.

Outside of that and the further east you go the more difficult it becomes. For example, in the current scam of HMRC tax fraud, which is one of the biggest trends in fraud, we see the funds going out to China through iTunes vouchers. That is much more challenging for us at the moment.

Q263 **Douglas Ross:** How do you deal with those challenges? You are going to say, "This is a difficult one to solve; it is not Europe; it is not the US where we have a good relationship". When you say, "This is a new scam; this is what is coming along; this is what is affecting our constituents and the people in the UK", how do you deal with the more difficult scams in areas where we do not have such good relationships?

T/Commander Clark: In each one we take what we call a 4P approach under the organised crime strategy 2016: what are the pursue options, what are the protect options, what are the prevent options and what are the prepare options? We work across each one of those 4Ps with a 4P plan. With the more challenging ones we work with our overseas liaison officers and our contacts, with the National Crime Agency and HMRC who have overseas liaison officers, and we put requests out for assistance. We also work through letters of request in overseas jurisdictions, which can be slow and untimely.

Q264 **Douglas Ross:** Do you think that is the best method?

T/Commander Clark: Those are the recognised legal methods through the legislation that we have. We also look at complete alternatives, for example disruption. Disruption sometimes is more effective to stop future fraud. Even if we cannot detect or are slow to detect the fraud that has taken place in the first place, one of our main priorities is to stop it continuing. One of the first actions we take with online shopping fraud and internet-based fraud is look to see if there is a disruption option available to us.

Q265 **Will Quince:** We have touched on Action Fraud. There is some concern that chief constables consider that they have handed over all the responsibility for fraud-related matters to Action Fraud. What do you think are the key responsibilities of local police forces in relation to investigating and recording online fraud in particular?

T/Commander Clark: Each local force area operates in autonomy, with its PCC and chief constable setting the local policing plan, based on the

priority setting of that local force area, its population and the fraud that it records and sees daily, for a strategic assessment and a control strategy. Their duty on reporting types of fraud is to recognise that there is a national structure, a national reporting centre. As I said earlier in response to another question, that does not stop them taking responsibility at local level for investigating fraud where it sits and fits squarely on their force area or the regional collaboration of the forces in that area. They are required to record that centrally and get an Action Fraud number so that we have a national crime recording number that is accountable to the Home Office, essentially. They are required and mandated to report their outcomes as and when they get an outcome for the crimes that they are investigating on their force areas.

Their other responsibility is for vulnerability and victim care locally and that is a responsibility undertaken by chiefs in their own force areas. It may be that they care for victims of investigations that are not owned by them on their force area. For example, Greater Manchester would be caring for victims because they are citizens who reside in their force area but the investigation might be in a completely different force area, and that is the anomaly of fraud.

Q266 **Will Quince:** I appreciate what you say about priorities being a force-by-force decision, but given the impact that significant fraud, online or in other ways, can have on an individual, do you think enough forces treat it as a high priority?

T/Commander Clark: I think historically, no. An enormous amount of work has gone into changing that by myself in the National Co-ordinator's office through what we call crime business areas in policing and through the Home Office and very recently through the Minister for Security who has written at my request to all chief constables in all force areas asking them to recognise the seriousness and priority setting that there should be in investigating fraud and online fraud. I have also worked with the Home Office to achieve the Home Secretary commissioning Her Majesty's Inspector of Constabulary in 2018 to inspect local forces on their counter-fraud response.

My job is to work with them and improve the standard of investigation and the recognition of fraud at local level. We have recently published a "Blackstone's Practical Policing" guide so that every force has an investigation model best practice way of recognising and going about countering fraud in their areas across those 4P plans. We work on achieving additional funding, for example for the rollout of an Economic Crime Victim Care Unit, which was piloted in London last year and is about to be launched in Greater Manchester and West Midlands police in 2018. There are significant steps and improvements at both the policing level and through political intervention taking place to improve the priority setting at the local level of chiefs.

I have also interrogated—I suppose is the best way of putting it—each force on whether they have a contact direct to Action Fraud on the force

website. It started out at 28; I have now improved that to 42. The only one that does not hold it is a force whose website is being upgraded at the moment. I have looked at 29 different forces providing peer support to improve their counter-fraud responses. We have worked with the College of Policing to recognise fraud investigation as a professional practice area of specialist capability. There are a number of streams. I am held to account by the Director General and through the Joint Fraud Taskforce in that respect and in my work.

Q267 **Will Quince:** Before I ask the same question to Detective Superintendent Porter, could you give us a rough indication of what proportion of cases reported to both police and Action Fraud result in an active line of inquiry being pursued and then the follow-up if that is the case?

T/Commander Clark: You may have missed it earlier, but 25% of what comes in goes out for active inquiry.

Q268 **Will Quince:** What does that mean? That was my question: what does an active inquiry mean? We all get these constituents' letters with an Action Fraud letter that look like diddly-squat has been done, quite frankly. For any other crime if you had reported, "My car has been stolen, my house has been burgled" and you just got a letter back saying, "Sorry, there is not really much evidence we can follow. Sorry you have lost 20 grand but it is kind of tough, isn't it"—and that is the kind of letter they get, and we have had an example read out—that is not an active line of inquiry as our constituents would see it.

T/Commander Clark: Where it is recognised that a traditional—as we would recognise traditional—investigation to pursue an offender and feel a collar should take place, 25% of what is reported goes out of NFIB for that traditional investigation at local or even national level. That is the National Fraud Intelligence Bureau assessing the case as viable to put police resources into investigating to make an arrest, if that makes it clearer to you. That is not to say, as I said earlier, that that is the only action that would be viable for action. That would also fall into the category of removing a website, seizing a bank account, taking a telephone number down. That is active police pursue in stopping the fraud but not necessarily arresting an offender. There are different methods of active police work in fraud, but about 25% of what comes in goes out for traditional investigation and is deemed viable to find an offender and arrest them.

Detective Superintendent Porter: What that looks like in Manchester is it is a real challenge investigating fraud because of the volume. There are some challenges in how we communicate to the public where we prioritise our resources. Everybody on this panel will know what the impact of fraud is on victims, but when you are prioritising resources against other competing demands such as child sexual exploitation and other expectations that the public have of our resourcing, there are some difficult questions around fraud and how we commit to that. On the disseminations from Action Fraud, in Manchester last year we

investigated 4% of those crimes in terms of a traditional—and while that might seem a shocking statistic, the reality is a capacity issue for us. We have to make some really difficult decisions based on threat, risk and harm.

The model that we are looking at in Manchester at the moment is how we support those who are most vulnerable. We have had some additional funding so that we have a researcher, an analyst, and we will prioritise our investigations against certain fraud types: the types of fraud where the offender is present, the bogus traders, over 65s, romance fraud and some other vulnerability reports from the bank and financial institution SARs reports. We will give an enhanced level of service to any victims who fall within those categories but that still leaves a huge area of demand that we cannot service in a way that we would like to because there are positive lines of inquiry.

Some of the challenges are around the fact that our fraud is cyber-enabled or phones have to be examined, so there is a huge amount of activity in investigative capacity. Of the 190 investigations my Economic Crime team currently has live, 50 are over 12 months. It is not just the scale; it is the length of time some of these investigations take through traditional investigative means. Some of the options of disrupt and other options for investigating fraud are probably where we are at now.

One of the other interesting things that we have been looking at is local offenders. We took a sample of offenders in Manchester over the summer and looked at, in terms of threat locally, how many of those offenders are known for domestic abuse or sexual offences and are we going to target those offenders as opposed to other offences that ordinarily we would want to investigate if we had the resources, but we have to make those difficult decisions. Of the offenders that we looked at, 7% of our fraudsters had domestic abuse markers and 7% were known for sexual offences. If we are making difficult decisions on resourcing locally, they are the areas that we are likely to prioritise.

Q269 **Will Quince:** Can I ask all of you one final question on that theme? Given the low risk, high reward nature of the crimes, what kind of message do you think it sends to criminals that this is not being treated as a high level priority? This is easy pickings for them, isn't it? I am not criticising you but you are confirming that the chances of getting caught are slim to none.

T/Commander Clark: It is certainly a challenge and my biggest challenge is making sure the police officers countrywide know the impact on the victim. If there is one message that I try to drive home permanently is the significant impact that fraud has on victims. It is not a victimless crime. There is a chance of catching the perpetrator more often than not on those crimes that are deemed viable for investigation and I need to change still more mindsets on prioritisation of fraud across UK policing. I think I am making significant progress and we are turning the corner, but it is slow and it is hard work.

It is about the victim and we should all remember what we are there for. Six out of 20 victims say that there is a significant impact on them, if not a devastating impact. The Economic Crime Victim Care Unit has been a big success in that respect. Last year it contacted 4,000 victims. These are victims who will not get an investigation. Out of the 4,000, only one became a repeat victim, which is a success in its own right in target-hardening our citizens, but it also stopped two suicides. That is worthwhile work. Not always just chasing the offender but the awareness message to our citizens and target-hardening them also has to be a path that I take.

Richard Piggin: The fact is that when consumers report an online fraud they expect action to be taken and often they are disappointed and frustrated when action is not taken. What I mean is that they are hoping that somebody, regardless of who they have reported it to, is out there looking to help them recover money, if they have lost it, and we are talking life-changing sums of money, as I said. They are hoping that someone will help them recover that money and identify the fraudster. They are disappointed, frustrated when they get a letter back a month later, two months later saying, "No viable leads have been found". It is particularly in online fraud when some of these victims have used that report to give what they think are clearly identifiable leads, whether that is a bank account number and a SORT code, sometimes a name and address of a fraudster who has not given them goods or services. They are thinking these are clearly identifiable leads that could be investigated and so it is disappointing when they get a letter back saying that no action has been taken.

The other point is on reporting of fraud. The consistent message is that the first port of call is to report the fraud to Action Fraud and yet speed is of the essence with some of the online fraud. As the Action Fraud website says, if your fraud has involved an online payment or transfer of money your first port of call should be to report it to the bank and most consumers will. If they have lost money, often they will first report it the bank and, regardless of where they report it, they are hoping that somebody will be taking action and looking into it on their behalf.

Katy Worobec: I have great sympathy with what the police have to try to cope with in dealing with the fraud problem. We work very closely with the City of London Police through our own Dedicated Card and Payment Crime Unit, which since it was set up in 2002 has had about 580 convictions. In 2016 that amounted to 124 years of sentencing, but it is the tip of the iceberg as far as dealing with organised criminality is concerned.

The key thing is that our focus is on all fronts. As well as looking at it from the point of view of the investigation, it is about trying to prevent and detect fraud at the front end and from the banking industry's perspective they prevent about £6 in every £10 of fraud every year. The target-hardening is really appropriate. It is about making sure that

potential victims are aware of what they can do to stop themselves falling victim in the first instance. It is crucial to make sure that people are aware of the types of scams that are out there, which are constantly changing, so that they do not fall victim in the first instance. We have our Take Five fraud prevention campaign running to try to raise that awareness and make people understand what they can do to prevent themselves falling victim.

It is also about partnership, in my view. It is about all the parties needing to be involved in working against the fraudsters. It is not just a policing problem or a banking problem; it is a problem that has to be dealt with by others like the telecommunications industry, the ISPs and so on. They need to be involved even if they are not actually losing the money or necessarily dealing with the victims.

T/Commander Clark: I am advocate of secure by design. As I said earlier, in a third of all fraud reports the key enabler to a person becoming a victim was the telephone. I think there are industries like the telecoms industry that could do more. We have the banking industry sitting on this panel. It does a significant amount. That is not to say it cannot do more but there are industries out there, new age industries, fintech industries, internet service providers, domain hosts, telecoms industry, where a huge amount of fraud is facilitated initially through those means. I think those industries could do more to help us on the Joint Fraud Taskforce.

Q270 **Chair:** Can I clarify some of the figures that we have had from you? Detective Superintendent Porter, you said about 4% of the cases reported to you. Was that cases that are investigated or lead to prosecution?

Detective Superintendent Porter: Investigated.

Q271 **Chair:** What proportion of the total leads to prosecution?

Detective Superintendent Porter: If I could send you the details of the exact outcomes afterwards.

Q272 **Chair:** That would be really helpful. Of the 100% of cases that are reported to you, is that just reports from the public or does that include the reports from Action Fraud?

Detective Superintendent Porter: That is everything.

Chair: That includes the reports from Action Fraud?

Detective Superintendent Porter: Yes.

Q273 **Chair:** Commander Clark, in the cases that you were talking about you used the figure of 25%. Could you clarify what that refers to?

T/Commander Clark: Crime reports into Action Fraud from members of the public and our business partnerships amount to 280,000 that are Home Office counting rule crimes. Of that 280,000, just over 71,000,

25%, are sent out for dissemination to pursue investigations. Outcomes are judicial and non-judicial that can be counted under the current rules and the return at the moment is about 14% outcomes.

Q274 **Chair:** Is that 14% of the 71,000?

T/Commander Clark: No, 14% of the 100%, which is the 280,000.

Chair: It is 14% of the 280,000?

T/Commander Clark: Correct, yes, in other words about half of those that are sent out. That is not including the disruption figures, which are the 170,000 requests for disruption of enabling services: telephone numbers, websites and e-mails.

Q275 **Chair:** You said that 14% leads to a judiciable outcome.

T/Commander Clark: Judicial or non-judicial outcome.

Chair: What might a non-judicial outcome include?

T/Commander Clark: Non-judicial could be a community action, for example a fine. It could be a restorative justice outcome as opposed to a charge.

Q276 **Chair:** Would you include the conclusion that it is not a crime at all as part of an outcome?

T/Commander Clark: No. It would go out as a crime but the outcome of the crime may not be judicial. It could be a fine instead of a court appearance or a restorative justice meeting as a resolution instead of a—

Q277 **Chair:** How many of the 170,000 requests for disruption do you think lead to action?

T/Commander Clark: I would have to write to the Committee in that respect.

Q278 **Chair:** That would be helpful. Detective Superintendent Porter, on the number of complaints that come to you, could you say again—I think you said this at the beginning—what proportion come from Action Fraud and what proportion come directly from people in Greater Manchester?

Detective Superintendent Porter: There is a crossover of that data. I would have to break that down for you, but roughly 800 to 1,000 are from Action Fraud where a victim is within GMP, but for offenders and offences it is around 500 a month. I would have to give you a report with a breakdown of that in a bit more detail.

Chair: Those figures do not sound to me like they add up. I would like to try to reconcile those. If the idea is that you are only investigating around 4% and there is a smaller proportion of those that lead to a conviction, but you are saying you still have 14% leading to an outcome, that does not sound right when you are only referring around 25% and so on in the first place.

Q279 **Stephen Doughty:** I would be interested to know how this compares to other forms of reported crime in leading to an outcome. Do you know what that is, by any chance?

T/Commander Clark: Not right across the board but, for example, sexual offences are lower than the outcome result for fraud, which I don't think is anything to brag about across policing. Burglary is about comparative to fraud in outcomes. Other offences may be higher, for example assault, where victim and offender are both known.

Q280 **Sarah Jones:** I have a question to follow up, which is of the 600,000—and it might be this is a separate number—I am trying to understand how many crimes are reported by victims and how many crimes are reported by banks, financial institutions, telecoms industries. How much proactive reporting is coming from them?

T/Commander Clark: I will try to be clear, I am sorry. Total contacts into the national centre are 600,000. Of those contacts, when you sort the wheat from the chaff, recordable crimes under Home Office accounting rules it is 280,000. In respect of proportion between individuals and businesses, the main reporting from businesses is through two pipelines that come directly into the National Fraud Intelligence Bureau. They are provided by Cifas and their membership—

Sarah Jones: Cifas is?

T/Commander Clark: Cifas is an acronym that does not really stand for anything these days, but it is a risk-based counter-fraud service that consumer goods, banks and other people providing financial services sign up to to deal with applications to see if they are fraudulent or not. It is a database that is held to check against for fraudulent applications. The greatest proportion of reporting is by Cifas and UK Finance and certainly more reporting in that way than there is by members or the public.

Sarah Jones: There is more than what number?

T/Commander Clark: I am not going to give you a percentage because I will get it wrong, but of the monthly reporting more is via Cifas and UK Finance than by members of the public. It probably outweighs it by two to one.

Q281 **Preet Kaur Gill:** Listening to the evidence thus far, it is quite clear that there is a great deal of complexity when you are investigating online fraud. Does the police force have the skills to investigate online fraud and should we have been recruiting specialist staff?

T/Commander Clark: There is progress in both areas. In terms of policing from bottom to top, through the College of Policing there is now recognition and specialist training courses in cyber-crime investigation and fraud investigation. There is also accreditation to recognise specialist fraud investigation in two parts. One is a bolt-on to what is the PIP accreditation for detectives in policing—that is the professionalising of the investigative process—at a number of different levels, investigator

through to senior investigating officer. There is also an accreditation that has now been held for many years, and that is for financial investigation, which ties into fraud investigation, so there are two types of accreditation depending on your specialist field. There are specific cyber and online investigation courses now run by the College of Policing and incentivised across all police forces in the UK for take-up.

Q282 **Preet Kaur Gill:** Do you know how many officers have done the training?

T/Commander Clark: What I do know is that the City of London Police has the National Economic Crime Academy. In the last 12 months it has trained staff from 25 of the 43 forces. Outside of London, I know that at my last national survey in 2016 there were around 800 specialist fraud investigators across UK police forces.

Q283 **Preet Kaur Gill:** Clearly there is still a lot more to do. I am thinking about the ability of officers, who are under a lot of pressure, to go and train. Is it about bringing in people with the specialised skills to work with officers? Is that a much better model? Has training made a difference?

T/Commander Clark: Training definitely has made a difference. To have fraud investigators recognised and rolled out as specialists is something that I would consider a significant achievement personally. I think that there is more to do on direct entry of specialist skills and I do not think that traditional policing recruitment has helped that. Again this is a strand that is being worked on at the moment between ourselves and the College of Policing and the National Police Chiefs' Council. Why wouldn't I take a specialist fraud investigator, who has done it for 20 years in a bank, who wants to come in and work in the police force?

We have increased volunteers in our sphere of work as well, and the ability of people to come in as not police officers but police investigators. The issue with that is their powers exist in local areas and we seek to change that so that they have national powers, the same as police officers would, up and down the UK. There are difficulties and complexities; there is work being done; there is more to do.

Q284 **Preet Kaur Gill:** Do you think it would be more effective for all online fraud investigation to be carried out at a regional or a national level as opposed to involving local forces?

T/Commander Clark: At every level there is a responsibility for countering fraud. At a local level, protection, victim support, victim care is absolutely the critical skill requirement. At regional level where organised crime groups are operating across country boundaries, there has been a significant improvement in policing since 2015 with the creation of regional fraud teams, but there is a lot of development required because they can get snowed under by taking three or four jobs of a size, veracity and complexity that maxes them out.

At a national level, as you know the Home Secretary announced an economic crime reform just pre-Christmas, at the back end of last year.

That is something that the City of London Police is partnering with the NCA, the FCA and HMRC in developing a national economic crime centre. I think that will make a significant improvement in upstream work and overseas work.

Q285 **Preet Kaur Gill:** Are there any specific changes to police resources and processes that you think could increase the proportion of cases of online fraud that result in prosecution?

T/Commander Clark: I think one of the biggest inhibitors at the moment is the disclosure burden in policing and especially with digital evidence. Digital evidence is vast, and I know from the cases that the City of London Police hold at the moment that it has 70 million pages for consideration of disclosure. The disclosure regime under CPIA legislation, Criminal Process and—I am trying to think what it stands for. I will come back to you on that. The burden of disclosure is huge and the burden to put disclosure together pre-charge means that there is a significant time delay in bringing offenders to charge and to justice.

Q286 **Chair:** Could you clarify what that 17 million referred to?

T/Commander Clark: 70 million is the pages that—

Chair: Seventeen or 70?

T/Commander Clark: Seventy. In the investigations being undertaken by the City of London Police now, somewhere between 500 and 700, the pages for consideration for disclosure pre-charge amount to 70 million.

Q287 **Chair:** That is across all of those cases?

T/Commander Clark: Across all of those cases. That is a significant burden that keeps police away and ties them down pre-charge before they even get an offender to court. I think a reform of CPIA rules and disclosure is required.

Q288 **Preet Kaur Gill:** Has there been any review of that?

T/Commander Clark: The last review was in 2014, which did not deal with the matters that I am speaking about. It was a review of disclosure rules.

Q289 **Preet Kaur Gill:** Were there any outcomes as a result of that review or any proposed changes?

T/Commander Clark: There were, but not that would significantly assist in fraud investigation.

Preet Kaur Gill: That is really interesting. Just the level of resource that would be required to even get through—

T/Commander Clark: Yes. The other thing for me would be pre-charge victim care as a business-as-usual within policing, as opposed to just post-charge victim care. In fraud, if you investigate for three years and you lose your victim, it is too late by the time you get post-charge victim

care. I think a remodelling of victim care services to provide pre-charge victim care is a worthwhile effort.

Q290 **Preet Kaur Gill:** The HMIC assessment in 2015 highlighted the concerns about victim support. Do you think there have been changes since that report in ensuring that especially local forces are doing that and working with the NFIB and fraud investigation during that process? I appreciate it is a long time.

T/Commander Clark: I think volume has outstripped any recommendation and implementation of the time that you speak of and I think it is time to look again. ECVCU, Economic Crime Victim Care Unit, as a concept that is, as I said, piloted in London, proves the concept for me that pre-charge victim care is essential and that funding should be made available to that. I would go one further to say that the sustainability of funding is really important to effect strategy and make a difference in online fraud investigation, and one-year allocation of budgets does not help.

Q291 **Preet Kaur Gill:** Have you had a reduction or an increase?

T/Commander Clark: I have had a 5% reduction, and in year, in fact, of policing budgets, and I have had no increase over the last three years. It is not necessarily always about the amount of money, although no public servant would not want to be in receipt of more, because you can do more with more. I feel as though we have done more with the same, to the point of taking on a 30% increase in reporting without any extra money and in fact a 5% reduction in real terms. But it is not always about the volume and the amount of money; it is about the sustainability of that budget agreement and arrangement. When you are working on 12 months, it does not help. I would like to see three- to five-year budget arrangements.

Q292 **Preet Kaur Gill:** My last point about police resources is that the National Audit Office in 2016 said that the main function of one in six police officers was neighbourhood policing whereas there were fewer than 150 police officers devoted to economic crime. Is this an appropriate use of police resource?

T/Commander Clark: I certainly would not disagree with the figures. In terms of the appropriateness, I still think there is a job to be done at community level in protecting citizens from fraud, so I would include some of their role at local level on community policing as being a fraud role.

Q293 **Chair:** Detective Superintendent Porter, do you want to comment on that?

Detective Superintendent Porter: Yes. What we are understanding in Manchester and the funding that we have had to look at vulnerable victims and the threat posed by some of our offenders, I agree that we need to have an understanding at a local level. It is a very specialist area

and we have benefited, certainly locally, from the Action Fraud model, ECVCU, taking up some of the victim care for the victims who are in Manchester but the offence may have been committed elsewhere.

It feels as if it needs to have some national response to fraud because of the jurisdiction issues. In protecting frontline resources, not all of our investigations require warranted powers, so I think there is more that we could do in terms of looking at different options. We are working with universities in Manchester and with academics on some of our cyber-crime issues. I think there could be more of a partnership response and perhaps more of a national response for some of the volume fraud issues.

Q294 **Chair:** Do you think there should be a complete restructuring of the way this works, 43 different forces all doing a little bit compared to some sort of regional or national change?

Detective Superintendent Porter: Yes, it feels like that, certainly for us in Manchester, in terms of resource. Frequently there is no release valve for us. While there is a response regionally, it is a very small team, so they can become overwhelmed with large cases very quickly. You are then left with the option of, "We can't investigate that" and it sits locally, which is giving a poor service. It feels like there needs to be a look at the restructure.

Q295 **Chair:** How would you restructure it, ideally? Put the funding issues aside and let's suppose the funding issues were magically being taken care of by the Home Office, how would you restructure it to be able to get the best and most effective investigations? Would you do that nationally, regionally, locally or what mix?

Detective Superintendent Porter: I think there is a combination. There is something around the central Action Fraud being able to disseminate all the intelligence and pick up on things and trends. I know from a local perspective, looking at our victim hub, that 20% of our vulnerable victims are out of our force. There is the postcode lottery. We are offering enhanced service and other forces may not. I think there is something more regional and being able to support that response with technology so that we are not going up against our colleagues on threat, risk and harm. When we are looking at examining computers and phones locally, that is also against our colleagues who are investigating murders, sexual exploitation. In terms of threat, risk and harm, fraud is then put to the bottom of the list of priorities. Having a national service with some regional hub-and-spoke models would feel like we could gain some capacity.

Q296 **Chair:** You are talking from the point of view of one of the biggest forces. Obviously for smaller forces that would be even more the case. Would you have it so you had local victim support but then entirely national and regional investigations?

Detective Superintendent Porter: For the majority of online, yes. I think the local policing response is around that threat, risk and harm,

who are the offenders who are posing the most threat, fraudsters, overlaying some of that data, and who are our vulnerable victims who may have other issues and we need to support. I think that is very much a local policing response and we need to own that.

There are also some real challenges in that 70% of our victims are businesses, so what is our partnership arrangement with businesses? We want Manchester to be a place for businesses to thrive. If 70% of our victims are businesses, they are not necessarily going to meet that vulnerability threshold but we know that if small businesses are victims of fraud, people are going to lose their jobs. I look at that as a demand area where we were not really effective at the moment.

Q297 **Chair:** Would you put it into City of London or into the NCA?

Detective Superintendent Porter: City of London has that level of expertise around fraud, so I would see it as being the hub of fraud and economic crime, but I think it needs an investment nationally in a different type of service.

Q298 **Chair:** Commander Clark, we are either boosting your empire or increasing your workload, effectively. What is your response to this?

T/Commander Clark: I think there has to be a national standardised approach, specifically in reporting, recording and accountability, with a national investigation capability that takes on the most impacting economic crimes that affect the wellbeing and infrastructure of this country and its credibility as a financial hub above all else with transparency globally.

There is certainly a case for growing regional investigation. That is a case that I am making through the Police Chiefs' Council daily. I would have regional investigations as the main structure in this space, with the local services providing essentially victim care and local policing responsibilities whereby victim, offender and location are in the same place.

Q299 **Chair:** Before we move on to the wider industry issues and prevention issues, can I ask you, Mr Piggin and Ms Worobec, for your perspectives on the policing operations, the way they work at the moment and what you would do to change things?

Katy Worobec: I have a great deal of sympathy with what has been said thus far. Looking at our own Dedicated Card and Payment Crime Unit and the way that works, I think there is a case for using that model of partnership working. If you were to have a more centralised approach to fraud and economic crime, there is an opportunity to make use of the resources more effectively. The DCPCU works by having both the Met and City police officers working with industry experts as part of the unit. That is its strength and it allows a better understanding of what is going on and makes the investigation much richer.

If you were to replicate that sort of model more centrally, you have an opportunity to take resources from the industry, working with the police in a much more structured way. Similarly, if you look at the Joint Money Laundering Intelligence Taskforce, you have the model where the National Crime Agency is working with the banking industry to gather intelligence and use that by working together. There are some models that I think you could build on to make use of resources right across the partnerships more effective.

Richard Piggin: Which? only has the experience of consumers and we have not looked at the structure of the police, their response, the models, processes and resources they have. What I am hearing is that there are a lot of significant challenges to responding to fraud once it has happened. Which? has looked at the role of preventing fraud and focusing on what people can do to prevent the fraud from happening in the first place. One significant concern that we have is that far too much emphasis is being placed on consumers to simply protect themselves, when we think there are others in that fraud journey who are much better placed to manage the risk.

Q300 **Chair:** We will come on to that next. Can I ask you a follow-up to Preet's question about victim support? Do you have any further perspective on what support there should be for consumers and for victims?

Richard Piggin: Victim Support—and it sits on the Joint Fraud Taskforce—does a good job working with those who have fallen victim to fraud. The consumer expectation again is that someone is there looking out for them. That is the most important thing. That is the key for them, whether it is from a local policing perspective or from victim support.

Q301 **Sarah Jones:** Going back to something that was said earlier about how it all works, just to clarify, because we are looking at quite a complex model that the National Audit Office did about how you report things, and there is no role for the local police force at the starting point in that model. It basically says somebody reports it to the local police and the local police report it to Action Fraud, Action Fraud looks at it, takes a view, and might report it back. You said a couple of times that there is nothing to stop the local police force from taking action in this model. As it is drawn, that is not there. It is clearly a complex system that is not quite getting reported to us correctly, one way or another, so it is probably very difficult for an individual to understand how to do it as well. A thought might be that the NAO thing was wrong.

I want to ask about the other side, what you, Mr Piggin, started referring to, which is what more we can be doing as industries, the banking industry and some of the other sectors that you mentioned, the telecoms and internet companies. If you could expand a bit more, what do you think they should be doing to prevent fraud from happening in the first place? Then the same question to you: what more do you think could be done by your members to prevent fraud from happening in the first place?

Sorry, that is a very long question. There are similarities, to me, when we took evidence from the internet service providers, on crime online. The debate started with internet service providers saying it is down to individuals to report if they see something wrong, but where we have shifted to is, "No, it is not, it is down to the service providers to be proactive and remove it in the first place". There are some similarities with this issue. Could you go first on what some of the action could be?

Richard Piggin: First, I should say that of course consumers should be taking reasonable steps to protect themselves. Organisations like Which? provide lots of information and advice on how to spot scams and the steps that people can take. The point I want to make is that, given how sophisticated some of this fraud is and what we have, and the ever-changing nature of the fraud, we think that consumers are not best placed to manage that risk. Then you look at the other people involved. We focused on banks, but it is not just banks, it is other companies involved as well, enablers of fraud perhaps.

From the banks' perspective we are beginning to see some really good progress. There are far more prominent warnings placed on their websites when you are making online banking transfers, which is a positive step. We would be keen to see some evidence of the impact and how effective those messages really are in preventing fraud. Katy might well talk about the banking protocol. That is a good example of where joint work between banks and law enforcement has prevented fraud from taking place in bank branches. That is good.

Part of the essence of our super-complaint on bank transfer fraud was we felt banks could be doing more to spot fraud, identify where there could be suspicious or unusual payments. There was a payment of £300,000 mentioned earlier. I would expect that to be an unusual payment either out of one account or into another account. Banks are often better placed then the consumers to know what the fraud is and identify and use their data in the systems and all the data they have available to them to potentially intervene at some point to prevent the customer from losing money.

As I said, we are seeing some good progress. One particular live direction is proposals for a contingent reimbursement scheme, where if a consumer has been tricked into transferring money to a fraudster and they have not acted negligently, they would have the ability to claim that money back from the banks. That proposal is being suggested by the regulator. It could be in place as early as the end of this year. There is some more work that needs to be done on that, but we see that as quite a critical thing that banks could be putting in place to protect their customers.

If we look further afield, I mentioned before that Which? has looked into holiday accommodation fraud, holiday letting fraud. We did an investigation and tried to find how easy it was to place a fake listing on popular websites—Airbnb for example—that encouraged a user to operate

outside of the Airbnb secure system, which is how these fraudsters operate. We managed to place 16 fake listings using several different fake profiles across a number of sites, so we found it was relatively easy. We even managed to include information that prompted users to contact us outside of the secure system, to make payment and to enquire further, all these things that we would expect the platforms to be spotting and taking down. There was inconsistency in when they were spotted, what was allowed through and what was not allowed through.

Then when we reported our own fake listings to the committees, there was again inconsistencies in how quickly those listings were removed. One of the sites removed them within hours. One of the other sites took 13 days for our fake listing, after we had reported it as being fraudulent, to be taken down.

Q302 **Chair:** Which one was that?

Richard Piggin: That was Airbnb. There was a whole investigation. I would be happy to share the coverage of that investigation review.

The final point is on telecoms companies. Others have made a very good point about their role and their involvement. Right at the end of last year we looked at an issue of text spoofing. This is another type of fraud that we have seen where, if you receive a text message from your bank, you often will not get the message come from a number, you will get it coming from a short code. It will be the name of the bank. It will be Barclays or NatWest or Lloyds and it will appear on your phone as from Barclays or NatWest or Lloyds.

There is readily available technology that enables anyone to send a text message to your phone so that it appears as if it has come from your bank. Which? did this. We found the technology and we did it. We managed to send text messages to people's phones and they appeared in same thread as genuine messages from banks. It is very difficult for the consumer to spot whether that is a genuine text message from the bank, a fraudulent text message. That is where we think there are opportunities for telecoms companies to work with banks and others to tackle the systemic vulnerabilities that are in these systems, which could do a lot to prevent fraud from happening in the first place.

Katy Worobec: I mentioned earlier that the financial sector stops about £6 in every £10 of attempted fraud in a year, so there is a lot of work going on behind the scenes that maybe is not visible in the first instance. Individual organisations will be looking at transaction analysis for unusual spending, to look at things like whether the information is being sent from the same IP address as you would normally send your banking work from, as an example, or they are looking at things like voice biometrics. There is a whole range of things in place. That said, I think there is a lot of work going on in that space.

The challenge that you have with particularly the types of authorised push payment fraud that is causing the issue is that it is much more difficult to identify what is an unusual transaction in these sorts of circumstances. If you are looking at card transactions, you can build up a profile of the way that people spend and the way they use their cards on a regular basis. If you are based in Manchester and you use your card a lot in Sainsbury's and not very much anywhere else, you can build a picture of what that particular cardholder is and does. Then if a transaction suddenly occurs at an ATM in Thailand, unusually, there is an opportunity to intervene.

The trouble with the types of transactions we are talking about is often they are one-off. As an example, £300,000 sounds like a high value transaction, but to some people that is not a high value transaction. At the end of the day, it is the customer who is making the payment from one account to another legitimate account. It is very difficult to spot those in flight and do something about it readily.

Nevertheless, we are working on trying to do that. I think what would really help would be a better legislative framework to allow quicker and better intelligence sharing between the banks and with law enforcement. We have asked Government to enforce new powers to help with that. There is a lot of intelligence sharing already within the industry on confirmed fraud. Once you get into the strains of the money-laundering world, you get some quite difficult challenges because you have to submit suspicious activity reports and you get into a world of pain on that. I think if we were to have clearer powers to allow banks to share information that would help to protect customers much more readily.

On the issue of helping customers to help themselves, I think that has a part to play, because people do get caught out. These fraudsters are constantly changing the way that they manipulate and scam people. You mentioned the banking protocol as an example of where, in the real world, in the solid world, we are able to work with police, victim support and Trading Standards to help victims go into branches and identify when they are going to make withdrawals, and hopefully make very successful—to the tune of about £9 million prevented from being taken out of victims' accounts as a result of that. The partnership approach is very much one that we need to follow.

The final point I would like to make is to echo the point about the need to bring other parties to the table, the telecoms industry, people like the ISPs and others. I have always wondered, for example, why we have to pay extra for security software when we purchase our computers and devices. Why is that not installed right at the outset? Why do we have to pay extra for it as consumers? If we can, perhaps with the Joint Fraud Taskforce, bring some of the other players to the table and say, "We really need your co-operation to help with the enablers of fraud", that would make a difference in helping victims.

Q303 **Sarah Jones:** Can you respond on the point about refunding victims of fraud? Obviously there are two ways of looking at it. If you stop £6 in every £10, it means you enable £4. Therefore, there is an enabling that goes on that people have called out in Which?, but other campaigns, *The Telegraph* Money, which say that banks are able to shrug off responsibility for having offered their services to criminals. David Clark has said that victims should take banks to court on the ground that they have facilitated the crime by allowing accounts to be opened in the first place. There is a counter-argument that says you are not doing anywhere near enough and you should be doing more, and if you are not doing more you should be giving the money back to the victims because it is certainly not their fault. You have the money, so why don't you give them their money?

Katy Worobec: There are a lot of things in that. I will try to unpick some of them if I can. On the opening of accounts, as I mentioned earlier the banks are bound to do their KYC checks—know your customer checks—and the FCA police that. They are very clear what they have to do when they are opening accounts. There is a conflict because banks have to open basic bank accounts, so there is a tension between having to make accounts available but still having to provide the KYC checks.

Part of the issue, as I said earlier, around that is that accounts are often taken over by fraudsters or used by fraudster rather than it being a problem with account opening at the outset. It is about, again, educating people not to unwittingly become money mules, which we have found to be an issue. Students, for example, are targeted by fraudsters to earn money by becoming money mules. There is some education work to do there to say, "Do not allow your account to be used in this way because it is allowing money laundering". That is becoming an issue as well. That is around the account-opening piece.

In terms of the refunds to victims, we are looking at ways in which we can chase the money more effectively. It is about looking at how you can refund victims, but for me it is also making sure that we do not just stop refunding victims of these authorised frauds, because what I am keen to ensure is that we do not allow the fraudster to be the only winner in all this. We do have to try to follow the money and to get that back as well as refunding the innocent victims.

Q304 **Sarah Jones:** Do you think you should refund innocent victims or not? I am not clear.

Katy Worobec: We are working on looking at the PSR recommendations about the contingent liability model that Richard mentioned. It is a question of making that work effectively, but I think it has to be done within the context of a scheme that is looking at trying to get the money back from the fraudsters as well as refunding victims at the outset. I think it has to be a mix of both, otherwise the fraudster is the only winner.

Q305 **Sarah Jones:** Do you think that with the naming and shaming approach that has been suggested banks and other organisations would suddenly change their behaviour? Do you think that would encourage a change of behaviour?

Richard Piggin: To some extent there is already some naming and shaming. For example, we look at banks' different security systems; we rate them; we publish papers on them to give consumers information about choices they might want to make when opening a bank account. To some extent there is.

There is an interesting question as to whether there is some level of data that could be published about fraudulent accounts that are opened by banks. We have been a little bit concerned by the FCA's proposal that one of the measures that banks should start publishing is how quickly and easily they open bank accounts. On the one hand consumers do want to be able to open bank accounts quickly and easily, but we do not think that should be at the expense of security checks that banks should be putting in place to make sure that the person opening the account is who they say they are, and monitoring that account to make sure that it is not being used for fraudulent purposes. Perhaps there is some consideration and balance there that you could publish alongside the account-opening statistics about how quickly you can do it, some data on the number of fraudulent accounts that have been opened or have been operated through a bank.

Q306 **Stuart C. McDonald:** I think we had got almost all the way through the evidence session before we first heard mention of the Home Office's Joint Fraud Taskforce. Is that because it has been ineffective? What has it achieved and what should it be trying to achieve?

Katy Worobec: I have been involved with the Joint Fraud Taskforce since its inception and I think it has made some inroads. The banking protocol piece, for example, is one of the things that we are operating under the Joint Fraud Taskforce. One of the challenges is to try to get Government law enforcement and industry to understand each other's issues, as much as anything. That has certainly been part of the challenge that we have had.

That said, I think there is more the Joint Fraud Taskforce could be doing. Probably what we need to do is to bring some of the other participants that we talked about earlier—the telecoms industry to name but one—to the table to have a more strategic and holistic look at the issue of tackling this kind of volume crime, because it is not something that anybody can tackle in isolation. It must be done in partnership. I think that is the key thing for me.

If I could go back to the transparency point, I am not a great fan of the idea of publishing league tables of which bank this week has the most fraud, if that is what is being—

Chair: That is not unsurprising, given your job.

Katy Worobec: I am not sure it is particularly helpful. Having worked in the industry a good number of years, I have seen the way in which the industry shares its intelligence between banks. For me, that is much more important. What it does not take account of, in looking at what any individual bank might be suffering at any particular day, is what other people are doing outside the banking industry that is causing the fraud. Data breaches, for example, where a customer's financial data is exposed by somebody who is completely not the banking industry might be causing fraud for customers with a particular bank. You have to think about whether that is going to be really helpful. Plus, fraud does tend to move very quickly. Fraudsters will target a particular vulnerability one week and another the next.

I am not sure that it is even in the customer's best interest to know what this league table looks like. I think it is more about being able to have a good conversation with law enforcement and making sure that the intelligence the industry has is shared with law enforcement to greater effect.

Q307 **Stuart C. McDonald:** Mr Piggin, what are your thoughts on the effectiveness of the contribution that has been made by the Joint Fraud Taskforce, if you have any at all?

Richard Piggin: It is quite insightful that you have to ask the question, to be honest. We are almost two years since the taskforce has been established and for us it is still unclear what impact the taskforce has had, and that is not good enough. We have raised concerns in the past about the transparency around the taskforce, what it is doing, what progress it is making, how effective some of the things that it has been doing have been in preventing fraud. All of the board minutes were published on one day last year, in October, so if you were so inclined you can read through all those minutes and build up a picture.

Stuart C. McDonald: That happened to coincide with the appearance before the Public Accounts Committees of the chair of the board.

Richard Piggin: It did. You can read through those minutes and build up a picture, but for us what the taskforce still has not done enough of is to demonstrate how effective it has been in tackling fraud. We did a survey of over 2,000 consumers in September last year and asked them to rate what should be the top three priorities for the Government. Up there at number 3 was tackling financial fraud and scams. It is a consumer priority; that is what they say. We have heard about the scale of it.

We were very supportive of the Joint Fraud Taskforce when it was established. We think it is recognising the right approach, collaborative, joined-up, utilising all the different information and all the different players. That is the right approach. We would still like to see more transparency, more publication of what it is doing. We would like to see an action plan of what the taskforce is doing, what its objectives are,

what its priorities are and then what progress it is making against those, a regular report so we can see how effective—like the banking protocols. That is a really good example; you can read it in the minutes. Katy will talk about it and I have heard about it. The banking protocol is a really good example of work that is being done where there is the clear impact it has had in preventing and tackling fraud.

We want to see what has been the impact of some of the other things that they have been doing, the impact of awareness-raising campaigns for example. There is a lot talked about them. We want to see how effective they have been in preventing fraud and protecting consumers from losing money. That is the sort of thing we would like to see.

Q308 **Chair:** Just a couple of final questions, and can I thank you for the generosity of your time? We appreciate how long the session has taken. We would appreciate some clarity on the figures, because they do not add up currently. We may be misunderstanding, but looking through the figures that you have given us, if the GMP figures are both accurate and typical of forces around the country, the Action Fraud figures should be about half the level of those that you gave us for the number that lead to investigation, never mind an outcome. It would be helpful to get a reconciliation of those.

Let me ask you finally where does this go from here, the next two years, the next five years. If we carry on with the approach to resources, structures and policies that we have at the moment, what do you anticipate happening over, say, the next five years on online fraud, given that at the moment it looks as though you have about 95% of cases that are being reported still not being investigated, never mind leading to any kind of conviction or outcome? Katy Worobec, do you want to start?

Katy Worobec: Is your question if we did nothing what would help us?

Chair: If we carry on with what we are doing at the moment. If we carry on with the current approach, what do you anticipate happening over the next five years?

Katy Worobec: I think there are a few things from our perspective that are coming into play. There is regulation through the payment services directive that will bring in stronger authentication. That is already on its way in. That would make a difference to some of the fraud that we are seeing. I think the work that is already in train to try to tackle things like the push payment scams will begin to make an impact. There is letting some of the things start to bed in. I think that we need to make some changes to the legislative framework to allow better intelligence sharing. I believe that is what we need to crack for getting better outcomes.

Q309 **Chair:** If I may just push you a little bit. From sitting here listening to all the evidence, it sounds like we have a massive escalation of these crimes taking place and not a massive escalation of comparable response. It sounds like we are way behind having any chance of keeping up with this. There may be some worthy and sensible things that are going to be

happening, but how do they compare with the scale of what you would anticipate the increase in crime to be over the next five years?

Detective Superintendent Porter: There are real challenges of resourcing. We cannot continue the way that we are operating around investigating fraud. What we will do is create a fertile area for more criminals to diversify into because the chances of being caught are slim unless it hits certain specific criteria. There are some real concerns about that.

In terms of demand increasing, the banking protocol and the collaboration with the financial industry is great but that in itself is creating a demand on policing. The GMP has about 30,000 suspicious activity reports a year from the banks. How we work together to tackle this I think has to be a priority in taking it forward. I would like to see a national service, going forward.

Richard Piggin: I think that fraudsters will evolve; the methods with which they try to con people out of money will change and respond to changing technologies and changing services that often are intended to benefit consumers. Bank transfer fraud would not have existed 10 years ago. Airbnb and holiday accommodation fraud would not have existed a few years ago. It will evolve.

I am confident that some of the things that Katy said about the measures that banks are putting in place to check the account number matches the account name, the reimbursement scheme, should have an impact on tackling bank transfer fraud, which should be great. That might mean that fraudsters will evolve and look at what other systemic vulnerabilities or loopholes they might exploit, so we have to be aware of what they might be and look at potentially some predictive policy around what that might look like.

That also raises the question of the other companies that are involved, those enablers and what responsibility they have and what responsibility they should be taking now to protect their customers. That is what we need to see happening, otherwise fraudsters will just change their route of attack.

T/Commander Clark: I have a shopping list. I may have to write to the Committee, I think.

Chair: Give us the top couple of things on the shopping list and then write to us.

T/Commander Clark: A huge focus is on post-offence response from the Committee today and I think people in general. I would much rather look at what is sustainable for a strategy and look back at cause and effect. If we look back at things like data theft and data breach, a huge amount and percentage of fraud results from way back when the data was stolen. The whack-a-mole effect that police play in trying to keep it

down is not sustainable and nor is short-term funding arrangements for that sustainability. I have said that more than once today.

We need to look right back at cause and effect. That is secure by design. It is making sure that companies do not store data on a cost-over-security basis in a third-world country that has lower demands and standards placed upon it in keeping millions and millions of individuals' personal details, and that is what happening.

We need to make sure that the citizens know what the place of our legislation is, that is ban cold calling. If you ban cold calling, you do not necessarily have to enforce it. Citizens just need to know that it is illegal. We have debated for a year and a half as to whether we should ban cold calling for pensions. Ban cold calling for the whole lot. There is no requirement to cold call anyone. They are two of the big things.

I do not like to be threat diagnostic in that respect. I like to see the bigger picture. A central register of bank accounts would help my officers, Greater Manchester police officers and other officers across the country get fraud investigation quicker because they would not have to rely on banks coming two weeks later to answer, and banks would not have to put resources into data protection authority requests. We would be able to look at the central bank register for accounts and we would be able to identify where the suspect account is. I would publish the suspect accounts that are made available to the national reporting centre for fraud. If a bank account is made available, or is 10 times, for example, across those 600,000 contacts, I would publish it. It will make the banks take action, it will mean that there is a warning list for citizens to check against and it will mean that action is taken.

Identity crime is not a crime in the UK. The theft of data and the theft of somebody's identity is not recognised as a criminal offence in the UK, but that is where most fraud results from. However, there has been good change and we are in a trajectory of good change. The Criminal Finances Act, the beneficial ownership register are all extra tools in the fraud investigator's bag to help. The FCA regulation of binary options in 2018 is a huge step of taking that out as a commodity in terms of investment fraud. There is a trajectory of good things and good impact happening.

Q310 **Chair:** A final very short question to you. Do write to us with other proposals that you have if you have them, but if we do not do all of those things, what happens?

T/Commander Clark: Then we will continue with short-term vision, short-term strategies, we will continue to play whack-a-mole, but we will make incremental progress that is slower than it should be.

Chair: Thank you very much. I thank all of our witnesses today. We appreciate your time and the evidence that you have given us.