Online Crime Working Group – 27 November 2014

Transcript of Item 5 – Online Crime – Second Part of Question and Answer Session

Roger Evans AM (Chairman): We will start our next session, which is with our police witnesses: Rebecca Lawrence, Director of Strategy from the Mayor's Office for Policing and Crime (MOPAC), Detective Superintendent Jayne Snelgrove from the MPS, and Commander Steve Head, who we met yesterday and who is the National Police Co-ordinator for Economic Crime at the City of London Police. That was a very useful session we had yesterday.

Jennette Arnold OBE AM: Yes, excellent.

Roger Evans AM (Chairman): However, we were left with the impression that we were really only scratching the surface and we could quite happily come back for another session if we have questions outstanding at the end.

Our first questions are about the current situation and working together and they are in the hands of Joanne.

Joanne McCartney AM: Yes, they are quite general questions and we will have some more detailed ones shortly. Perhaps I can start with you, Commander Head, if I may. Could you just briefly outline to us what role the City of London Police has in tackling online theft and fraud and what role does the MPS have and how do you actually work together?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): It is an interesting development and it is a development that has happened over the last three years as a response to the emergent nature of how crime is changing.

Effectively, the City of London Police is the national lead force for fraud and we host the National Fraud Intelligence Bureau (NFIB) and now we also host Action Fraud. I believe that you saw the NFIB yesterday. The role there is to take all of the crime reports for all of the country and to bring those into one place so that, for the first time, we are able to recognise the true picture of how criminality is happening right across the country. The representative from the BBA recently talked about the international dimension and that is also very much highlighted by bringing all of those crimes into one place. Rather than looking at them in isolation and thinking, "There are some crimes in Lincolnshire and some crimes in London", we can see how they are linked and connected. We then send out those packages where we talk about enforcement to the MPS and the MPS obviously has its responsibility to investigate those crimes. We also furnish all of the details of victims to the MPS so that they know all of the victims in their areas, as we do for all forces around the country. Then we try to work with forces with our expertise and with the units we have to try to make sure that the response is as good as it possibly can be.

Joanne McCartney AM: OK. Thank you for that. With regards to Action Fraud, how would you rate its success so far?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): We took over responsibility for Action Fraud on 1 April this year and we have made a number of significant improvements to how victims are treated in relation to that experience, if you will. What I would say about

Action Fraud that it is really important as somebody who has been in fraud investigation for a little while is that that central reporting was really important. It was long overdue. As crimes happened on the internet, criminals and criminal behaviour changed and we needed a response that was fit for the current threat and the emerging threat. Action Fraud was the beginning of that process of us bringing it all into one place.

It would be fair to say that it is a brand new concept for policing and it has had its challenges. We hope that the things that we have done since 1 April have improved it. We have certainly tried to make much clearer to the victims of crime what is going to happen to the crimes that they report. We have tried to be far more open and transparent. We have worked with Victim Support to try to pass on those messages in a way that is sympathetic to people's needs. Actually, we try to recognise the vulnerabilities - and there was some talk earlier about different parts of society being targeted by different frauds, particularly the elderly - and try to work with those groups that work with the elderly to make that a better experience.

I was saying that there are still improvements needed. I would still like to think that we could get the message of Action Fraud out there in a far better fashion. I would like more people to know about Action Fraud and to know what it can do and how to report it. However, we are improving in that sense and things are much better than they have been previously.

Joanne McCartney AM: Before that, it was quite a fragmented system, I believe. Is that right?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): It was extremely fragmented. There is an HMIC report out today that talks about policing keeping up with the modern world. We all live our lives on the internet now or most of us do and that is just a fundamental way that our lives have changed, mostly for the better, out of the development of technology. Policing needs to keep up with that change of technologies, criminal methodologies and criminal behaviours. The idea of bringing all crimes into one place has been an important step forward, recognising that crime does not happen as it used to. The fact that we can target tens of thousands or hundreds of thousands of people instantaneously over the internet and be geographically remote from them has changed the nature of crime. It has changed the nature of the threat we face. The systems that we are putting into place now are a response to that and that is why they are important.

Joanne McCartney AM: Thank you. With regards to Action Fraud, perhaps I could turn to Detective Superintendent Snelgrove. What is the MPS's view of how well Action Fraud has worked?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Until recently, the MPS had not properly engaged with Action Fraud and we had a disperate relationship in relation to the crimes that were being reported in from Action Fraud and how the process worked. Since we have set up FALCON, we have been able to establish a very strong relationship.

Actually, for us it is essential that the Action Fraud process works both for victims of crime and also for police forces around the country. We are investing a lot of resources into responding to cybercrime and fraud. However, the role that Action Fraud plays allows us to focus those resources on the investigation of crime and not the initial reporting of crime. We get crimes sent to us from Action Fraud that have some ability for policing to investigate a viable line of inquiry and the locus of the investigation has been clarified and so, ultimately, there is action that the MPS can physically take. That means I can direct my officers in the right areas. If we had no Action Fraud process, we would be spending a lot of time reporting crime from victims and also, actually, it may be that another force or even a law enforcement agency overseas would be better placed to actually investigate that crime and that negotiation would also be quite costly in terms of resourcing. For

us, it has helped in terms of aggregating crimes together and passing them to the right force that is most likely to make the best sort of impact in that crime area.

Joanne McCartney AM: Given that you said there is a benefit to having Action Fraud, can I ask why the MPS is setting up volume crime hubs? I have a quote from you to say that you are setting them up because:

> *"... one weakness was that we were not responding to the volume of crimes being reported through Action Fraud and into the MPS."*

Can you just clarify? Are your crime hubs going to be hubs that members of the public can directly report crimes to? If they are, is that not replicating or duplicating what Action Fraud is meant to do?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): No, I was slightly misquoted. The volume crime hubs have been set up as part of FALCON to deal with the volume crime offences that are reported in to us from Action Fraud to ensure that there is actually a policing response once the referral comes into the MPS.

Joanne McCartney AM: That clears up that quote, then. Perhaps I can turn to Rebecca. The Deputy Mayor for Policing and Crime has been on record as criticising Action Fraud, calling it 'No Further Action Fraud'. What are MOPAC's concerns about the system at the minute?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): MOPAC has carried out a lot of consultation, as you know, and has done a lot of work in this area in conjunction with law enforcement colleagues and we have found a number of things.

We have found that the issues for individual customers can be quite different from business customers for the very reasons that your questioning earlier, Caroline, suggested. Individual retail customers if they are refunded often do not experience this as a crime or suffer loss in the same way as business customers. What we heard in our work on business crime consistently - and Police and Crime Commissioners and in fact Ministers hear this as well - is that businesses are dissatisfied and have been dissatisfied with the overall response to fraud. This is not to lay blame. It is just the changing nature of crime.

In particular, they heard that the Action Fraud systems and structures would not allow these bulk reports from the larger businesses and they were cumbersome to use. You have heard from our two law enforcement partners there some really positive news and that is now being changed. Businesses told us that when they report fraud, they often do not hear anything back. Again, you have heard from Commander Head that some real improvements are being put in place. Also, crucially, the reporting systems and the process chain do not necessarily maximise the chances of forms of detection. If you were to look at a decision-making tree, there are lots of points at which it is difficult for an investigation to progress.

It is fair to say we have had very good joint partnership working and there is a really renewed focus on this area. We are encouraged by some of the improvements to the systems that are being put in place. However, we really need to keep an eye to make sure that this area of law enforcement serves the needs of the public.

Joanne McCartney AM: That was very helpful. Commander Head, we were told yesterday that the bulk reporting is going live very shortly. Is that right?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): It is absolutely right. Bulk reporting is really important for us in terms of maximising the opportunities for big

business to report to us. We accept that there is under-reporting. In fact, I was very interested in the previous conversations around the importance of getting as many reports into the system as we possibly can. Only by having those reports do we have the very best intelligence to use and give those best enforcement opportunities, if you will.

I will just say that it is really important that we are able to give an across-the-range service. We need to be really responsive to the needs of individuals, quite often vulnerable individuals who call the system, as well as SMEs and large businesses. We are trying to do that in a very graduated fashion. It would be fair to say we really tried to concentrate in those early days on the most vulnerable in our communities. We are glad to say that we are now around to bulk reporting, which will be coming in at the beginning of next month, on 5 or 6 December 2014.

Joanne McCartney AM: Thank you. I understood that there was due to be a review of Action Fraud but that the funding was taken away and that did not take place. Is there planned to be a review or should there be one?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): We do our own reviews on Action Fraud, as you can imagine, and we do an awful lot of that. We have put in a bid for an extensive review not just of Action Fraud but, now that it is connected to the end-to-end system, the Action Fraud portals, the NFIB which takes some fraud and cybercrime reporting and the mechanisms for feeding out into forces. We are going to do a review of all of that process from beginning to end. As my colleagues have explained, it is that end-to-end service that is the really important part of it. It is the enforcement aspect. It is the disruption. It is the work that we can do with the data feeds that we have and the big data that will lead to the really effective prevention campaigns in future.

Joanne McCartney AM: That was very helpful. Thank you. We are going to have some questions later on about victims and FALCON, but perhaps I can just clarify with Detective Superintendent Snelgrove. Will the volume crime hubs sit under the FALCON Command or are they separate?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): No, they are part of FALCON. If I can explain, FALCON is bringing together the MPS's response to fraud and acquisitive cybercrime all the way from the low-level auction site fraud that you may experience through to complex cybercrime and complex fraud inquiries.

The reason we have done that is it has enabled us to have officers who may be less experienced nurtured and brought through by those who are investigating those complex offences. In terms of the investigative response to a series of auction frauds on the internet, for example, it may not require significant technical understanding, but it is actually linking up bank accounts, email addresses and methodologies to identify perpetrators. However, some of these will have the odd piece of technical infrastructure with them in terms of using perhaps proxy servers to hide identities, which officers may not have experienced before. What we are trying to put in place is a buddying network system whereby those officers who are very highly trained and who deal with these sorts of investigations at a very complex level can support their junior colleagues.

Therefore, in terms of FALCON, we will have volume hubs based in four London locations so that they can deal with victims and perpetrators of crime in a local environment. They will be linked into the Organised Crime Command in terms of the complex fraud and cybercrime, but also key to this is having a prevention team that works with all of those officers so that we can look at where we have linked series of crimes and look at the enablers of those crimes and see what we can do to actually target those enablers, whether that is just awareness for the public or working with businesses and industries to try to design them out.

Joanne McCartney AM: Thank you for that. I know my colleagues have some further questions later on. My last question to you all is really asking you where the gaps are with regards to working with other organisations. What could the police do a bit better? Do you have trouble getting certain organisations on board? We heard earlier that the banking sector is coming to talk to the FALCON Command next week, but where are the gaps and what could you do better?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): I do not think there are any gaps in terms of appetite. Most businesses and most other law enforcement departments and agencies that we talk to are very supportive and see that there has been a gap in relation to our response and want to work with us. The issue for us actually is trying to manage that in a realistic sense and also make sure that we are keeping grounded in relation to getting on with enforcement and prevention work on a day-to-day basis.

We are starting to create networks of industry that can help us in terms of cybercrime and so we know who to go to for help with the very complex offences and help with unlocking some of the evidence that we perhaps may struggle with from a technical perspective. We are also developing very key relationships with the banking sector. Financial Fraud Action UK (FFA UK) also provides an umbrella response to crimes affecting the banking industry and we work very closely with them and also with individual banks. We are also dealing with a lot of retailers who are suffering online crime. Actually, for them it is basic fraud that is just being perpetrated in volume over the internet and we are starting to understand their business processes and to work with them on a daily basis.

The issue for policing is how to maximise the intelligence that they can help us with and how to manage that on a mass scale. That is where NFIB greatly assists us in being able to be the depository and analysis centre for all of that bulk data, allowing forces like ours to then be able to see the wood for the trees in relation to investigations.

Joanne McCartney AM: OK. Thank you.

Roger Evans AM (Chairman): Commander Head, you mentioned a review of Action Fraud. Could you just tell us when that it is going to be?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): It will be at the beginning of next year. I am hoping that it will be before 1 April 2015.

Roger Evans AM (Chairman): All right. Thank you for that. We have a number of questions about how victims are supported.

Jennette Arnold OBE AM: I have some specific questions and then a general question, but I just want to start off with a few comments. Three of the five Members on this Working Group are victims or have been victims and a number of us have been repeat victims. As well as this being an issue, we believe, from what we have heard, and an area of importance to Londoners, this is one area where Assembly Members are part of that experience.

We have heard that many victims - and we have experienced it, as I said - of online banking fraud have this weird experience because they do not experience the material loss. As we heard from our representative from the banking sector this morning, they are refunded by their bank. It seems to us that this leads to a perception that people worry less about crime committed online than they do about traditional crime.

However, we heard at our previous meeting from Professor Mark Dutton from the University of Portsmouth. His research showed that victims of online crime can be just as distraught as traditional victims. Even though they had not lost any money, some of the victims said it was just their horror and the mere thought that somebody had impersonated them and there was that invasion and identity loss. It was as important or as traumatic as, if you like, a mugging or physical contact.

My question is to Detective Superintendent Snelgrove. Does the MPS appreciate that or does the MPS have a different perception about online theft and fraud and see it as a set of criminal activities that Londoners are less worried about and in fact you can place less priority on it?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Absolutely, we understand that and even more so now that we are dealing with victims on a large scale and listening to their stories.

At an induction day that we held here, my new officers who were being trained up and being given the vision and strategy for FALCON heard from a woman who had been a victim of an online dating scam. She was in her 60s. She explained that she had recently been divorced from her husband and that she was having a new lease of life and embracing her retirement. She was financially secure and she felt that she wanted to create a larger social network. She met an individual online and over a series of many months she lost over £80,000 to this man. She explained to us that, yes, the financial loss was significant to her because it was part of her life savings and it was her financial security, but what was more important to her was the fact that she became so depressed. She felt she could not trust anyone. She felt that she had been stupid. She was embarrassed. She got so low that she almost considered suicide. When my officers were listening to that victim of crime, you could have heard a pin drop in the room. The reason I put that lady – and she was very brave to do it – in front of my officers was to explain to them that this is not a victimless crime.

That is one of countless stories. It might be someone who is phoned up and gives across their banking details and has money taken from their account. Yes, often they are refunded, but they feel as duped as somebody who gets burgled in relation to an artifice burglary, for example. They feel that they are on top of their game. They feel like they are not that stupid and that they will not become a victim. Then they are and it is almost like pulling the rug from underneath them. It has a massive impact on them personally. We do understand that and we do treat every victim with as much care and sensitivity as you would expect us to.

Jennette Arnold OBE AM: You can say that for your specialised teams, but to what degree and how much more work do you have to do to get that kind of perception and understanding to the front desk of the boroughs? You are a long way away from that, are you not?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): We are. We have to be realistic. The reason we set up FALCON was so that we could focus resources and make sure that all of the Action Fraud reports as of 1 December 2014 will come into a FALCON team. Therefore, if anyone reports via Action Fraud, they will get a response from an officer who has had that kind of training and input. However, if someone is calling 999 or 101 or walking into a front counter, they will get the officer that is in front of them. That is a challenge for us to make sure that we can give everybody that same level of input. That is my responsibility. I am not just in charge of FALCON; I am responsible for fraud and cybercrime in London and getting that message through is critical.

Ultimately, I would expect officers to be giving a victim of fraud or cybercrime the same level of care as if they had been mugged, as you said, or suffered a burglary or any other type of crime. That is the basic level of policing I would expect, even if they had not had that specialist input about the impacts of fraud.

Jennette Arnold OBE AM: To follow on, are you in the middle of mapping incidences so that you will soon be able to tell whether it is much more prevalent in one part of London or in certain boroughs and that kind of intelligence? Are you in the midst of that or have you yet to do that?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): We are supported by the NFIB, which provides the intelligence analysis of what is going on in London in terms of how many reports of crime and what the intelligence picture looks like and that can be as granular as postcodes. What we are also doing is looking at the crimes that are coming into the FALCON hubs. We understand that we have more offences northeast and east of London, oddly, than we do in the west at the moment. We need to understand why that is before we react to it. It could just be a current trend that will not be replicated in 12 months' time or it may be because there are particular methodologies targeting the particular types of people across London. That is something we are looking at. We need to understand why people become victims and what we can do to make them more secure and safe and if there is anything that they can do in addition to what they have in place now.

Jennette Arnold OBE AM: I asked that because that knowledge is essential if you are going to provide personalised support. Because of the complexity and the diversity of London's population, you cannot really take a one-size fix to victims. You need an intelligent base to understand how to advise about victim support.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Absolutely, and it is not just that the victims may be different but the methodology employed by the fraudster will also target a particular person. If it is an investment fraud, for example, it may be a very different victim than if it is online dating fraud or potentially an eBay auction fraud over match tickets, for example. Frauds basically look at who has money, who we can target to get that money and what is most likely to work. Ultimately, anyone, as you have said, can be a victim. The methodology employed may be slightly different and therefore my job is to make sure that people in London realise that they could be a victim and getting that message that resonates with them. We find that we put out lots of messages and people only really listen when they become a victim of crime, not before they have become a victim. It is very important to us to try to work out how we get the message across before they are a victim.

Jennette Arnold OBE AM: Lovely, thank you. I will come back to you in a moment. Can I just ask Commander Steve Head how the City of London's Economic Crime Victim Care Unit will work with the MPS to provide a joint service to victims of online crime in London?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): We see the new unit as a really important element about trying to make things considerably better, particularly for vulnerable victims.

My colleague from the MPS has described how we can break down in terms of intelligence what the picture looks like for victimology right across London. I can tell you that there were 40,000 reports last year and we can break it down to postcodes. That is data. It does not tell you about the people who sit underneath that and there is no humanity in that. What we have developed with this new system is a joint unit. There are officers from the MPS sitting in that unit. There are representatives of the British Transport Police in that unit and the City of London Police. All of the forces that police London are represented and we are working with Victim Support.

The important thing about that is that it will recognise the vulnerable victims that come through Action Fraud and it will try to provide a personalised service for those individuals. It is a limited resource. It is about 10

people or 12 people at the moment and obviously there will be a challenge in terms of doing that, but it is a really important step forward and that is taking it away even from communities.

Fraud is a global phenomenon. You have heard that from previous people giving evidence. The impact of fraud is felt very locally, in communities here in London, as it is right across this country by individuals, some of whom are very vulnerable. We have been able to develop responses to that which are no longer just national responses. We do not talk about the 'national picture' so much; we try to break that down into what that looks like for forces and what that looks like for individual areas.

All police forces in this country have invested a lot of money over the last ten years in developing community teams that understand their local communities. It is trying to take the messages that we see and feeding those in to those community teams, whether they are police officers or whether they are other teams that are working through the Police and Crime Commissioners or other bodies like that. The unit, hopefully, will take the most vulnerable and will be providing a very personal service to those individuals.

Jennette Arnold OBE AM: That is excellent. Thank you very much. From me personally, I would just like to feedback publicly just how inspired I was from meeting your team, especially the head. I am having an elderly moment here; I cannot remember his name.

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): If I can help, it is Peter O'Doherty [Director, NFIB and Action Fraud].

Jennette Arnold OBE AM: Peter O'Doherty, yes. He is absolutely fabulous. Do take back my commendations in terms of the work he is doing.

Rebecca, I have a question to MOPAC. You could look at it as an opportunity here because our work is very timely. Why I say that is that we know that it is early days for MOPAC, in a sense, in that the office has just only assumed responsibility as the commissioner of victim support services for London. That started in October. I would also like to put on record – and do correct me if I am wrong – that MOPAC has a budget of £6.7 million to commission victim support services. If you can confirm or correct me on that, it would be good.

Can you tell us about the plans that you have in front of you if this is a lead area for MOPAC? Will MOPAC be commissioning support for victims specifically of online crime in London?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Absolutely, Jennette, and you are right that your review is very timely and very welcome. It is an excellent issue to be looking into at this time. We worked with the City of London on its bid for the Economic Crime Victim Care Unit and so we are supportive of that. There was a Ministry of Justice competed fund and that has the funding for this year. We will look at the demands on that unit and we expect those demands to grow. We will need to take decisions about funding in the next financial year. That will depend whether there is another competed fund from the Ministry of Justice and we move to the same approach or whether we use our core victims allocation. However, we are absolutely mindful that victims of crimes committed digitally – as you heard from the very powerful example from Jayne [Snelgrove] there – experience these crimes in a very profound way and they deserve victim services. Therefore, absolutely that can be built into commission plans going forward.

Jennette Arnold OBE AM: In a way, as a provider, both of you have funds.

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes.

Jennette Arnold OBE AM: Is it part of this £6.7 million that you are saying funds the unit?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): I will have to come back to you with the precise number for the victims' allocation but, yes, our victims' provision for the coming financial years in areas of this crime is provided through the City of London Police. In the next financial year we will look at whether we do that again through the City of London Police and increase the funding or whether we complement that with other types of directly commissioned support.

Jennette Arnold OBE AM: That is all that you have to date in the MOPAC plans regarding support for victims of online crime?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Commander Head has his own opinion, but we were very pleased with the amount of funding.

Jennette Arnold OBE AM: No, I was asking about MOPAC because you are the commissioner and you have the fund.

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes, we have a fund which we are happy at this stage can meet the demand coming into our system. If it does not, we will look to commission additional services.

Jennette Arnold OBE AM: OK. I wonder if we could do it then by writing. I know it is early days and so what is the plan from October until the end of the financial year in terms of your spend and a programme from MOPAC regarding victim support for online? If you are still developing and having conversations, that is fine. I would just like to know. Have you made an allocation out of your victim support pot for online crime? If you cannot tell me today, then you can --

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): We have budgeted expenditure for this year of £260,000. It comes through the Economic Crime Victim Care Unit and that is a dedicated team that will work with the cohort of victims, as Commander Head has identified. The team has been trained by victim services through the best principles of victim services referral units. It will have victims referred to it by the City of London Police and British Transport Police and so it is a cross-London collaboration covering activities for this financial year.

It has quite clear criteria for referral where a case has been investigated by one of the partner forces and, if they are appropriate for a victims' package, then the victims are advised of this and referred through to that unit with a risk vulnerability matrix. That was the commissioning process for this type of victim care for this financial year, with funding for the project through to the end of March. Then we will do an analysis and a concluding report of what has worked and then identify what will be appropriate for the next financial year.

Jennette Arnold OBE AM: Thank you. At that level. Can I just take you then to a local level?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes.

Jennette Arnold OBE AM: The monitoring of victim care through the MOPAC model is taking place now at borough level through the Safer Neighbourhood Teams. What capacity do these volunteers - because they are Londoners who are involved in this - have? What support is there at local level if citizens arrive at their

meetings and they are victims? Have you thought through what support is needed at that local level? If you have, can you share that with us?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes, absolutely. If a crime has been recorded or experienced at a local level and it falls into this space, the referral criteria will apply. It will be a case covered by the MPS and people at a borough level will say, "Actually, there is specialist care here for victims of these types of fraud", who can experience the kind of disturbances that Jayne describes, loss of self-esteem, etc. It is quite specialist. The borough and the officers at the force level will be able to refer to the specialist services provided through this package of victim support though the City of London Police. It is precisely to help the local level understand when they might not have had experience of this and there is more specialist services available.

Jennette Arnold OBE AM: Yes. Thank you for that, but I just wanted to get a sense that - or I may have it wrong - there will be volunteers at the local level that will be listening and receiving these complaints. I can go off to my Safer Neighbourhood Board meeting and I could speak about my experience. Has MOPAC looked into that interaction and are they prepared to support those teams of volunteers? Where would they go with my concern if I turned up at my Safer Neighbourhood Board as a victim?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): I suppose that relies on awareness by the police and members of the Safer Neighbourhood Board of the services are there to support victims, but I would hope that the process we have undertaken of successfully bidding for a fund to establish these victim services and work across London on this would mean that people would know where to go. Officers within the Safer Neighbourhood Board structure could say, "Thank you for your concerns. We have some specialist services here that will be of use", and so they could refer on.

Jennette Arnold OBE AM: Maybe we can look at it in a different way: in terms of how you will be monitoring the work of these boards and what it is they pick up and how they deal with that.

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): You are absolutely right that the boards and the members of the board need to be aware of the services that are available so that people in boroughs can be well supported.

Jennette Arnold OBE AM: Yes, it is just at that point of where the victim is and where the conversations have been had. That has to be as positive at that point as it is anywhere else in the system.

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes, absolutely.

Jennette Arnold OBE AM: My last question to all is one of these open questions. What levels of support should the policing community offer to victims of online crime? Do you have anything to add to what we have heard or what you have said so far? It is just a general sweep-up question.

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): 'Online crime' is a really large generic term now and a lot of crime has an online element to it. I know that you had the College of Policing here earlier talking about training up policing. Policing needs to be able to deal with online crime because we lead our lives online and it is part of our everyday lives and it is, therefore, part of everyday crime. That is a fact and we need to catch up with that.

In the new systems that we have here and the new capacity and capability that the MPS are building, London is ahead of the curve in terms of what they are developing that meets not just the threat that we are facing

now but the threat that we know with emerging technology is just around the corner. We do accept that online victims are every bit as important as every other kind of victim and that we need to accept that and we need to make sure that our response reflects that understanding. That is not the case in every instance and my national responsibilities mean that I travel around the country and I see a mixed response sometimes. Sometimes it is disappointing, sometimes it is very pleasing, but that is where we need to be and that is where we need to go because online crime now is fundamentally just a way of life for us. We cannot see it as something that is entirely niche because it permeates every aspect of the crime we are looking at.

Jennette Arnold OBE AM: That is lovely. Thank you for that. Lastly, we heard from our communication team that you are due to launch something that we thought was very good in terms of informing members of the public and you are going to launch it on Friday. Is it something we know about and you do not?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): No. I would like to think there is nothing that they told you that I do not know about.

Jennette Arnold OBE AM: Just a test!

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): You can never be sure.

Joanne McCartney AM: They are in the audience watching.

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): Is it the Crimes of Christmas?

Jennette Arnold OBE AM: Yes.

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): The 12 Online Frauds at Christmas campaign. The MPS are linked into that and you will have seen it. In actual fact, of the 43 forces around the country, 39 are engaged with that campaign. It shows how widely understood now the theat is and how forces want to engage. This takes us back to the idea that you have a central repository of intelligence. We can actually describe what it looks like in the MPS areas down to borough level and across all of the other forces.

That campaign will not look the same if you are in different parts of the country. It will look distinctly different. It just depends on the needs of those communities. That has to be the future. We have to be far more intelligent and intelligence-led in the way we approach prevention campaigns in the future.

Jennette Arnold OBE AM: We will look forward to the launch tomorrow. Thank you.

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): A pleasure.

Roger Evans AM (Chairman): There are some questions about how FALCON is going to operate.

Tony Arbour AM: Detective Superintendent Snelgrove, you have already told us you have once been misquoted. Did you say when you spoke to the Cyber Security Summit last week that "having started working in fraud and cybercrime only at the beginning of 2014, you are none the wiser, really?" Did you say that?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Probably. There was probably a slightly longer sentence and so maybe you could give me the whole sentence. I was trying to explain to a large group of industry and academic colleagues about the nature of the threats in terms of the scale and also the fact that they are blended attacks and that my investigators need to make sure that they are looking across the piece, whether it be identity crime supporting email phishing campaigns, looking at hacking issues and then also the cashing-out money mule expertise that we have and managing the whole crime from end to end. I was probably being jovial at the start of my presentation. Often I tap the microphone and say, "I am the head of cybercrime", and I am not so good at turning it on. I feel my job is very much about raising the awareness amongst my colleagues and also externally about the challenges that we face. Certainly I definitely do not have all the answers and so I am probably being slightly self-effacing there.

Tony Arbour AM: I am pleased to hear that explanation. We often say that kind of thing. I am reminded of Ronald Reagan [former President, United States of America]. You will recall when at the beginning of his speech, which he did not know was being recorded, he said, "Let's bomb Russia". Do you remember?

However, there is a serious point relating to what you have said that relates to the learning curve. You have been in post some months and you have explained how complex the whole thing is. FALCON is recruiting very rapidly now and is expanding very fast.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): That is true.

Tony Arbour AM: That presumably means that most of the people that you are recruiting must be on this very, very steep learning curve. How are they coping?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): They are coping very well. We are accessing a lot of support and training. As I explained earlier, the model that we have put in place is seeking to use our more experienced investigators who look at complex offences to support some of the junior colleagues and those with less experience. One of the reasons for that is I do not want to find that investigations are closing because the officers think they have taken it as far as they can, as per their knowledge. I want them to take it as far as they can. They are two slightly separate things. Therefore, it is about making sure that the techniques and tactics we use for those complex investigations, if it is reasonable to do so, we can bring to bear on the lower level offences.

It is challenging because obviously there are large volumes. Officers in the volume hubs have over 1,000 separate investigations. Each of those has numerous victims attached and they have only started since August. There are a large number of investigations and when they need help they know where to go internally, but also we can access support from industry as well and we often do.

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): If I may add a small comment, we look across the MPS at where risk is. There is often risk when you build a new capability like this and you grow it very fast and you recruit a number of officers and you are doing something quite new. The leadership here has been excellent. If I may say so, the way Detective Superintendent Snelgrove has built this capability, the support she had had from senior colleagues and the way she has brought officers in, brought systems in and trained people up has been extremely impressive.

Tony Arbour AM: Related to that, do you not think that you might become victims of your own success? As there is greater awareness of the existence of FALCON and your 12 Online Frauds at Christmas campaign makes people more aware of this, might this not lead to - and perhaps it will be a very good thing - a very substantial increase in reporting as we have recently had in historic crimes and so on? You might, therefore,

become overwhelmed. Are you prepared for this? Is this part of your risk strategy for FALCON that a large number of complaints and increased reporting is going to occur?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Absolutely. It is one of our objectives to increase public confidence to report. There is certainly a feeling that victims were not reporting into the police, maybe to their bank but not the police, because they did not expect that we would be able to do anything about it or would be interested to do something about it.

The way we are managing the expectation - and it is already arriving, we are having more reports that we did this time last year - is there is a phased growth of FALCON. We have completed phase one and we have those resources in place. Phase two should be in place by the end of the financial year. At that stage we will take stock and look at where the resourcing is and what the demand looks like and then the Commissioner has given me licence to go back to the management board. Obviously, if I can justify the need for further resources, he will consider that requirement. That will be balanced on various other pressures, but the plan was certainly a three-phase plan and taking stock after phase two.

Tony Arbour AM: Is MOPAC prepared for this? We have an overall envelope of police resources and so on. When you say you have planned for it, I suspect it will be sudden as there is more and more publicity given to this. Even possibly what we are saying today in relation to this is going to mean vastly increased reporting. That is going to put pressure, is it not, on the whole of MOPAC's resources for funding the MPS?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Your point there is very well put. There is one very crucial piece in this space that we have not looked at this morning, which is the role of prevention and of designing out the crime and avoiding it being committed in the first place because in this area of online fraud it should be possible to design out the crime and prevent it at source through good information security advice and good uptake of that advice. One of the ways that we focus our strategy very much in response to that risk that you have said is by investing in building capability on that prevention side, where I have to say there is a huge appetite from the business sector to get involved.

You heard evidence from the colleague from Cifas who spoke to you, who has been very supportive of the Business Resilience Centre that we are setting up, which we are focusing on digital security and advice to SMEs. We have been really encouraged by the number of private sector partners who are contributing secondees and funding to set up that programme of information awareness, raising with really hands-on support to stop people becoming victims of this crime. You will not be able to enforce your way out of this crime. The Government Communications Headquarters has said 80% of these crimes are preventable. It is protective security of computer systems and awareness by businesses of what steps they can take to protect themselves that will get us ahead of the criminals here.

Tony Arbour AM: I hope you are right because I note that MOPAC does put this area of crime as part business crime, whereas the case cited by the Superintendent related to an individual case and my colleagues were all victims as individuals. Is it appropriate that MOPAC should only be dealing with this as part of business crime or should it be a more general thing?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Again, you raise a good point. The focus on bringing this issue as part of business crime does not mean it is only online crime experienced by businesses that we care about. We care through the strategies in the Police and Crime Plan about all types of victimisation. The point of the Business Crime Strategy was that where there are particular areas where it makes sense for law enforcement and for MOPAC and businesses to come together, it is a call to action, if you like, to identify some really specific areas which can galvanise action. The Business Crime

Strategy has allowed, for example, the Digital Security Centre to provide business resilience advice to SMEs to really shape and form in a way that we would not have been able to without the Business Crime Strategy. That does not mean we are not concerned by individual victims of digital crime. In fact, we are delighted that the FALCON capability can cover the full suite of types of crime that are enabled online.

If I perhaps could give you another example, we know that there is a spate of really nasty, horrible crimes increasingly committed online and that will be in the hate crime area. Victims of all those types that are targeted by hate crime are experiencing that increasingly online. There we would use MOPAC's Hate Crime Strategy to ensure that victims of hate crime receive the right kind of support and the perpetrators can be investigated and brought to justice, whether that crime is committed online or face-to-face. We take thematic strategies, but they will cover whether that crime is committed digitally or physically.

Tony Arbour AM: You are clearly right in that. I do not know how you categorise it, but there is an enormous amount of online harassment --

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Absolutely.

Tony Arbour AM: -- which currently is prosecuted in that way. I am not sure that there should not be some more generic thing which is related to this.

I was very struck, Superintendent, by MOPAC's view that prevention is an important strategy here in seeing that there is not a great deal of this crime. When we visited yesterday at the City we were told about disruption exercises, which I was quite struck by. I thought I could do a bit of that.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Yes.

Tony Arbour AM: Clearly there is a balance. If you are a victim you ring up and you want the matter investigated. You do not want it prevented because it has already happened. You do not want it disrupted because it has already happened. You want it investigated. There is clearly going to be a great difficulty which must happen in FALCON. How are you going to spread yourself? How do you prioritise these things? Indeed, to impress the taxpayers and indeed even to impress MOPAC who want to get the big offenders, might that not mean that you go for the very large fraud and you put your resources into that rather than dealing with the smaller cases which affect individuals?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): With FALCON, we have set up the opportunity to try to do both and we have a tasking process that allows us to apportion the resources appropriately. We have a central taskforce that is looking proactively at the organised crime groups that are operating in this environment. Often the intelligence is actually coming in from businesses. The large scale offences and the large scale offenders we are getting intelligence on from businesses and also from the NFIB to help us target who those are. We will put proactive - often covert - investigations around those individuals and try to tackle that high end. That is both for complex cybercrime and also for large scale frauds. Often there is an overlap.

The volume crime hubs are focusing on the individual crimes that are coming in and that may be a business crime or from an individual member of the public. Within the team is also a prevention unit, Operation Sterling. They used to predominantly focus on fraud and what they have always looked at is proactive prevention, what are the enablers for the crimes and how can we try to design them out. Now we have put additional resources into that team. The way they are being tasked is from an NFIB perspective: what are the most significant crimes affecting Londoners and London and what are the volume hubs seeing as the most

common methodologies that are used? Also in terms of the organised crime groups, how are they operating and what crimes are they committing? Using that information, we can then start to focus down on which bits of prevention activity we should be doing and how.

At the moment we are quite enforcement heavy still because particularly there has been a gap with the enforcement side. Businesses have told us that they know who is committing these things and how they are victims of crime on a daily basis but law enforcement has just not been interested in dealing with it. They have wanted an enforcement response. Individual victims of crime also expect that as well. We will see the balance slowly move as we become more effective in our prevention piece and much more intelligence-led. We will be able to assist in the designing out of the crimes.

We must recognise, however, that fraudsters evolve and every time we shut one door in relation to how a fraud is perpetrated another one opens. The issue of social engineering of victims is becoming more sophisticated. As you live your life online and you provide more and more information into the public arena about yourself it is easier for somebody who has never met you to make contact with you and gain your trust quite quickly and commit a fraud, despite all of the prevention advice, guidance and software security you may have in place. If you genuinely believe the person on the other end of the phone is a member of your family, someone calling from your bank or somebody who you work with, it is very difficult to design that crime out because that is human-to-human.

Tony Arbour AM: Can I ask who is responsible - it may not even be a police responsibility at all - if there was a substantial cyber attack? I can think of two scenarios. Is an Assange [Julian Assange, Editor-in-Chief, WikiLeaks] type thing when you get hundreds and hundreds of people simultaneously to have a go at the banks, say, or financial institutions, a police matter or is it a national security matter? Similarly, one which probably is a national security matter: I recall occasions when some of the small Baltic States have been completely taken out by concentrated cyber attack. Is that a police responsibility? Whose responsibility is it?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): I can say if you want. There is a series of responsibilities based upon the nature of the cyber attack that you describe. What I would say is that what we need is a response so that no matter where that attack comes into the intelligence, we have a cross-cutting ability. You will no doubt know about the Cyber Intelligence Sharing Partnership (CISP) and the work of the Cyber Emergency Response Team (CERT), which is a cross-government body, which obviously has representatives of the various security agencies as well as policing. They have a very large stake in terms of any of these things as well and we have seen them take action along with policing in relation to certain attacks on this country.

We have seen attacks on many of the institutions and the financial institutions. There is a police response that is required. Then the National Cybercrime Unit (NCCU) at the National Crime Agency we work very closely with. Only as recently as last week we were doing joint work with them on an attack that came into a number of what we would call critical institutions in the City.

The importance is that organisations like the NFIB, which you have heard about, we sit on those other bodies as well and they have links to our intelligence. The importance that that gives us is that, in actual fact, if one of these attacks comes in and it is not instantly recognised for what it is and it seems to be some other kind of attack, something much smaller, we have the facility to escalate that amongst our organisations in an automated way. That response is growing. We now sit as a full member of the CISP that I just mentioned before, and likewise they sit within the NFIB. Likewise, now we have people within the NCCU and various units and other forces.

It goes to the heart of the question that someone asked earlier on about where the challenges lie. There is a big challenge at the international level, a significant challenge. There is also a significant challenge at that volume crime level. They seem diametrically opposed, but they are not because part of the issue of the volume is the nature of the international attacks that we face. One of the things that I know that you will have seen and that we spoke about earlier is that element about disruptions. I noticed that the representative Matt Allen from the banks did not discuss this, but we work very closely with the banks in order to shut mule accounts, which what we would call accounts that are being used by international criminals to syphon money out of this country.

It is very difficult sometimes to target the criminal enterprise that lies behind this if they are in some of those more difficult-to-reach countries of the world, but we have to have a response that actually keeps people in this country safe and stops their money going. We do significant disruptions at that level with the bank and also with telephone companies - the voice over internet protocols (VOIP) - and even now a lot more with the internet companies themselves to try to do that disruption, predominantly from those threats that we face on an international basis. There is a lot more that we need to be able to do in terms of that international threat.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): If I can offer some level of additional assurance, the capability that Commander Head has sits within a national framework of civil contingencies. The Government as a whole through the Cabinet Office has a framework of assessing the hazards that the UK faces like flooding or extreme weather events or the threats it faces like terrorism and/or cyber attack. Cyber attack is a national level threat and that means there is a whole architecture of government that exists, both in terms of crisis response when Cabinet Office Briefing Room A (COBRA) is convened and there is a mechanism for each player rehearsing their response, but also that there are the law enforcement capabilities in place, which have been described by Commander Head, to tackle those threats. It does not mean that there is not a threat. In fact it is very much that there is, but there are mechanisms and structures and clear responsibilities in place.

Tony Arbour AM: I do not know whether I am relieved to hear that or not, but what does strike me is what Commander Head was saying. There are lots and lots of organisations dealing with this, both private and public. It is obvious that the banks and financial institutions will have their own 'police force', if you like, or their own 'FALCON'. I guess from what you are saying when you were talking about the big internet companies, the chances are that the big multinational internet companies have their own 'FALCONs' as well.

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): That is a really important point. The City of London is a really good example of somewhere where policing has a finite capacity within London and yet if you look at some of the really big global institutions they have far more resource dedicated to this kind of work than policing will ever put into it and they spend huge amounts of money on it. The importance is not trying to replicate what they are doing but to try to actually harness what they are doing and to make sure that we work in tandem with them.

Again, I do not know if it was mentioned from the gentleman from the BBA but we do a lot of work with the BBA to deliver dedicated cyber-enabled fraud training to their members. We understand the threat from both perspectives. We in fact have a common approach to it. If we are engaged in enforcement, then in fact as they prepare packages they understand those nuances of policing around things like disclosure and those sorts of things like that, which are important if we are to achieve enforcement results. Therefore, a huge proportion of what we do - and we have the National Fraud Academy now - is trying to make sure that we see commonality of approach and commonality of training across dedicated fraud resources, not just within policing and not just within other government bodies but across those kinds of organisations as well.

Tony Arbour AM: Thank you. It seems as though we are only scratching the surface, really, Chairman.

Roger Evans AM (Chairman): Indeed, and that is why we have a fairly tight set of terms and conditions for this Committee. Just going on to the objectives for FALCON, Detective Superintendent Snelgrove, what are you key performance indicators (KPIs)?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Our objectives are predominantly around improving the outcome rate for the Action Fraud referrals that we get in. In respect of that we looked at ensuring that we were, at least in the first instance, better than our most similar force because when we took on this challenge we were severely underperforming. We had an outcome rate of about 5% last year. We set a target of 35% this financial year because we have only been up and running since August and 50% for next year. That is basically ensuring that we are coming back to Action Fraud with a result of the investigations that have been passed to us.

Obviously, importantly, for us it is about making sure that we improve victim confidence in this area. That is always quite difficult to measure. One of the things I felt was quite critical, although I have talked about the fact that victims are affected in a lot of ways, is that with a lot of low-level offences it is about the victim getting their money back or at least law enforcement and banking and others trying to do everything we can to stop the fraudster getting it and securing it before it leaves the bank. We want to make sure that victims are compensated as much as possible. Obviously that is something that we have to do jointly with the courts, but that is another measure of success.

We are also looking to arrest more people - more fraudsters and more cyber criminals - and we are looking certainly in the first instance at a four-fold increase in the number of arrests and charges for those sorts of criminals. We are also looking at the organised crime element and ensuring that we disrupt more organised crime gangs. We have a whole suite of performance indicators that will help us measure whether we are making improvements in the right areas and that we are delivering against the objectives that we have set. They are the fundamental pieces that I am going to be measuring to ensure that we are trying to reach our overall objectives.

Roger Evans AM (Chairman): When you have those quantified, would you be able to write to the Committee and let us know what the indicators are that you are using?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Yes. I have those and I can send them when I --

Roger Evans AM (Chairman): All right. Thank you. Can I ask, Rebecca, if MOPAC is broadly in agreement with the indicators or are there other things that you are going to be asking for?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes, we especially did not set numerical targets in this area in our Business Crime Strategy because we know that reporting and confidence is an issue. We did not set numerical targets in other areas like hate crime or domestic abuse for similar reasons. We did say we want to see an increase in reported frauds and we want to see an increase in positive outcomes. It is for the FALCON unit to set those KPIs, but we are confident in the direction of travel they are taking and so that is the approach we have taken to measuring outcomes. Of course attitudes and confidence are also really important and this is under-measured and under-reported, which is why we have started and launched our Business Attitudes Survey in response to the very large amount of feedback that we had from businesses that they were not confident in law enforcement response. We felt that was an area we needed to be able measure and track so that we could get some real improvement.

Roger Evans AM (Chairman): Can I just be clear on the proportion of online thefts and fraud that currently have a positive outcome? You are saying it is 5%.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): No, that is not correct. Last year the outcome rate for the MPS was 5%. That is not positive outcomes. That is just outcomes.

Roger Evans AM (Chairman): That is positive and negative outcomes?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): That is positive and negative outcomes, yes. We expect to get at least 35% outcomes this year but the current rate is about 10% positive outcomes, albeit because we only started in August it takes some time for an investigation to actually come to a conclusion. We have had over 6,000 referrals from Action Fraud and a number of those are still under investigation and therefore the outcome has not been sent back yet. We currently have 10% and we expect that to significantly rise once the results are back through.

Roger Evans AM (Chairman): Your target of 35% is not unrealistic if you are achieving 10% now?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): No, it is not unrealistic.

Roger Evans AM (Chairman): Good. Rebecca, MOPAC is going to be publishing data for fraud committed against business as part of your business plan. Do you have plans to publish more material about fraud committed against individuals?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): No, we are publishing a business attitude survey, which is a complement to the public attitude survey and which asks questions about confidence in policing and using a similar methodology with a market research company conducting telephone interviews.

You raise a really good point in that there is not at the moment a consistent measure of the public's perception of online crime against individuals being an issue. There is quite an unusual system of reporting a police recorded crime here with reporting through a separate route from other types of crime, the reporting being through Action Fraud. It is a hugely technical area and it is covered quite well in the HMIC's recent report, *Crime Data Integrity*. The Office for National Statistics (ONS) is doing work here because countries across the world are struggling with the fact that their official recording systems of police-recorded crime and their victimisation surveys are not yet adequately capturing this.

We can look into whether we can amend our current surveys about where this could be asked. For example, we have an online survey for victims of sensitive crime that we are commissioning later this year, My Voice, and we can look at if we can add an online dimension there. There are national issues with which our country and countries across the world are struggling, quite frankly.

Roger Evans AM (Chairman): Can I just ask the MPS about the balance within the unit between warranted officers and civilian staff?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): In terms of the growth, we are growing by 154 officers and 38 police staff and we already had about 102 fraud and cybercrime police officers and then another 12 police staff supporting that. We only have a relatively small contingent - but we are looking to grow that if it is successful - of police staff investigators within the volume crime hubs and also

police staff technical investigators within the Complex Cybercrime Unit. What we are looking to do there is to create - and it was mentioned this morning for the College of Policing - a career pathway for police staff because we recognise the ability of bringing people into the organisation who may not want to be police officers but may have the skills that we want to develop. That pathway will potentially see them go one of two routes. They may just stay as a more omni competent basic investigator with cybercrime training or they may diverge into the financial investigator framework or into the technical cybercrime investigation framework. That gives them an opportunity for both lateral and upward progression within the organisation.

We do struggle, as has been commented on, to attract the right staff from a police staff perspective because of the pay scales and the way that the organisation sets itself up, but we do have lots of technical grades within the MPS that once members of staff are appropriately skilled and trained that they can move into. That is what FALCON is looking to develop once we have these core investigators.

What we do have within the MPS is a Digital Forensics Department, which has a lot of the technical skills. What we see as the challenge is making sure the people have the right balance of skills. You need to be technical but you also do need to be an investigator or you certainly need investigators and technical staff to work really hand-in-glove because they need to be able to interpret the information, put it to a suspect in interview, for example, and potentially even explain it to a jury in a court proceedings clearly and often in more layman's terms than a technical person can often achieve.

Roger Evans AM (Chairman): Warranted officers will all be detectives, yes?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Yes, there is a mixture. We have officers in the volume crime units that are police constables who are undertaking their training and becoming detectives. However, the majority of officers are detectives, yes.

Roger Evans AM (Chairman): Thank you. We have some questions which Joanne has about the challenges ahead. This is an area we have partially strayed into already, but there are a couple of things you need to mop up.

Joanne McCartney AM: Just following up to your questions, Roger, we know that the British Crime Survey is one that MOPAC is using to track confidence, for example. We have heard from our experts that the British Crime Survey does not actually have any detailed questions at all on online fraud in particular. Is it something you would welcome in the future if the British Crime Survey did actually have a set of questions in that related to this area?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): From a national perspective I would welcome that. Fraud is an important crime type. It is a growing crime type. The cyber enabler has brought it to people's attention, but it has been brought to people's attention because of the scale and the nature of the harm that we now face. It is important that it is included within those figures because that is where mainstream policing takes its figures from. That is not to say that the figures are not being held somewhere else because they are. It goes to the heart of what we see. I know that you talked earlier about the importance of reporting. I may have a different view from some who have put evidence forward, in that I support the idea of encouraging as much reporting as we possibly can and being as robust about encouraging that reporting as we possibly can. It is to the benefit of the whole country if we know that intelligence.

Joanne McCartney AM: Rebecca, is that something that MOPAC could lobby the Government for, for example?

Rebecca Lawrence (Director of Strategy, Mayor's Office for Policing and Crime): Yes, it is absolutely an area nationally that should be looked at. In London in MOPAC we have looked very hard a where the gaps are in the systems and we have created capability, be it security advice for SMEs or support to the MPS's capability, and we have introduced our own measurement systems for business confidence in London. However, it would really be worth developing the national framework here and really understanding what victims and the public are saying.

Joanne McCartney AM: Thank you. If I can move on to the future, I suppose my first question is to the MPS and also the City of London. What are the greatest challenges that FALCON will face in the future? Is it purely volume or are there other challenges that you are having sleepless nights over at the moment?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Volume is an issue for us in terms of working up digital evidence. It takes time to get digital evidence from computers and phones and to make sure that that is in a suitable format for presentation at court. That demand is only going to increase and we need to get systems in place to make sure that we are smart in terms of the devices that we seize at scenes, the ones that have evidence on them, and how we can provide best evidence at court without necessarily having to put restraining orders on servers that are in other countries, etc. Some of those legal challenges will be quite complicated. As we do this on volume, it is going to create a challenge.

The continual evolution of technology is something that certainly people like the College of Policing and other areas of policing are going to struggle to keep up with and we need to be very flexible and have a different approach to the training of officers and actually not necessarily think we have to have all of the expertise in one officer but that actually we have officers with a broad range of skills working together who may be experts in a particular device or a specific fraud methodology that can actually be directed towards the challenge when it comes. We also do need to be making sure that our training and also our access to advice and guidance from the industry is dynamic and that we can react to new technologies as they arrive and make sure they are not barriers to us investigating crime. It is challenging but there are a lot of people who are keen to support us. We are already getting a lot of our training externally at the moment to ensure that we have that up-to-date technical understanding.

Joanne McCartney AM: Is there anything you wish to add to that or is that it, then?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): I would reiterate those comments and I would just add that the challenge and the solution are the partnerships that we develop not just amongst law enforcement and not just a blend of skills amongst our own officers but right across the public and private sectors.

Volume will be a problem. We believe it is hugely under-reported. You have heard me say that I want to see more reporting and so volume will become more of a problem. In actual fact, the answers are out there in being more flexible about the way we deal with those challenges. Industry is investing an awful lot of money in this so we do not need to replicate in every instance that investment. We need to harness that investment and we need to work in a more cohesive fashion. That takes a big step forward by policing and we need to be bolder in the way we do that. In the past we have not always been good. It also takes a leap of trust and faith by big business on occasions. I would welcome some of the initiatives that have come from the banks. They have made giant strides but I would also say that there is an awful lot more that we can do together.

Joanne McCartney AM: If I can just ask - and Jennette [Arnold OBE AM] has asked this with regard to victims - about officers on the front desk, we have heard in the past particularly with regard to Twitter abuse,

for example, that victims often say that the officer at the front desk did not actually recognise it was a crime to start with or did not really see any interest in pursuing it further. Do you agree - and I suppose I am asking Detective Superintendent Snelgrove - that there is an issue with frontline officers giving this sort of crime a low priority, perhaps because they do not understand it?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): I do not think they are necessarily trying to make it a low priority but there is a skills gap in some of our staff around understanding how the crime is perpetrated and actually that a police response is needed. Obviously the College of Policing has been looking to mainstream the cybercrime training across frontline staff as well as specialist.

In the MPS with FALCON, although it would appear to be a specialist outfit, it really is trying to get a critical mass of officers who have that expertise at a more local level. They are not responsible in FALCON for investigating harassment kinds of offences but what they are there for is to support their frontline colleagues. They are based on boroughs and they can provide that support and guidance when you are looking at those investigations.

What that does not help with is that first interaction where the officer perhaps goes to a victim of burglary, for example, and that victim says, "By the way, can you help me? What should I put in terms of my security on my computer?" We cannot necessarily have officers who have expertise in everything, but what we need to make sure is that they know where to send the victim of crime or the member of the public who is asking for advice. It is those messages that I have to get out and it is not the case that every officer has that understanding at the moment, but that is certainly my ambition.

Joanne McCartney AM: What the College of Policing told us was that cybercrime or online crime is now part of the initial training package for new officers but that different police forces may do it as a whole block or link it to perhaps domestic violence and you might learn about an aspect of online crime with regard to that. Are you able to tell us today how the MPS is doing in training its new officers or, if not, are you able to write to us with that?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): I do have the details. What the MPS is doing at the moment is in terms of giving the whole mainstreaming side of a crime package. We focused on the FALCON frontline staff - the police constables (PCs) and the new detectives that have come into FALCON - to create that critical mass. The next step will be in making sure that that frontline staff has that training. I can send the figures. I have the details here.

What is also happening is every trainee investigator within the MPS has a cybercrime input within their development course and that is a three-day input on how to investigate cybercrime. Every new detective in the MPS will have that investigative understanding. We are obviously also adding specialist training to that and making sure that all of our officers have also done the National Centre for Applied Learning Technology (NCALT) online training package on fraud and cybercrime as well. There is a lot of work going on to try to upskill officers but there is also a lot to do and I can send the figures through afterwards.

Joanne McCartney AM: That would be helpful. Is it the case that younger officers - we call them the 'Xbox generation' - are more adept at picking up these skills quickly or not?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): They are, but there is also a need to actually train in what is behind the box. It is a little bit like car mechanics, is it not? Nowadays cars are more sophisticated and we are all probably used to them and families have one, two or three, but an officer knowing how they would actually work is probably less than 20 years ago. The thing now with the technology

is they are so intuitive and so easy and actually knowing what sits behind it and how you get evidence off of that device is the skill that an officer needs to have. They understand how people use it to communicate and they certainly know things like apps like WhatsApp and other things and how that is used. How they get the evidence off the device is still the critical training they need, but they are easier to mould and to train. Some of the most skilled cyber investigators are not young. They are experienced detectives who have been interested in this for a number of years and who have actually trained themselves both at work and away from work.

Joanne McCartney AM: Thank you. My last question is about the perpetrators. At our last session, we had one of our experts telling us, if I can quote:

> *"[The police] were saying you would be amazed at the people who are at it. They are middle-class, respectable people. There are midwives. In terms of buying, selling, marketing and so on, I think you will find a much wider spectrum of people getting into that [as opposed to traditional crime types]."*

I am just wondering if you are finding that the advent of the internet has made the opportunity of crime more open to a wider group of people or is it still mainly organised crime?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): It is probably too early for me to say. I have some anecdotal evidence and certainly the methodology of the crime certainly allows for a different profile. You do not have to have quite the same mentality to commit a crime over the internet as you would do potentially out on the streets and we do have anecdotal evidence of perhaps more women doing these sorts of offences but it is purely anecdotal at the moment.

One of the things that we do investigate though is insider threats and crimes happening within the workplace. Again, that is a demographic you find less obviously in other crime types, but that has been in fraud an issue for many, many years. Therefore, yes, you do get a very different perpetrator in those sorts of situations.

Joanne McCartney AM: Commander Head, do you have anything to add to that?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): I can say that in actual fact 'fraud' is a really broad term and in terms of the different kinds of fraud you see a completely different demographic. In terms of insurance fraud, you would be really surprised at the level of professional engagement within insurance fraud amongst the medical profession and all kinds of different professions. In mortgage fraud, you see a large number of professionals engaged.

However, that is not to say that serious organised crime has not infiltrated fraud, particularly cyber-enabled fraud, in a significant fashion. Quite often they will look to target professions or professionals-within-a-profession, if you will, in order to use them to support their commission of that fraud. Insurance fraud is a really good example where you get some really odious gangs that have been previously engaged in other kinds of criminality and that target doctors and other kinds of professionals in order to support that criminality.

Joanne McCartney AM: OK, thank you.

Jennette Arnold OBE AM: It comes from some stuff I was reading around the digital infrastructure and how some of the boroughs in the most deprived parts of London are least likely to be wired up and therefore accessing online services. In the borough represented by this gentleman to my right [Tony Arbour AM], Richmond, the percentage of the population there could be as high as 80% wired, whereas in one of my boroughs that I represent within the zone 1 area, the rate can fall as low as 30%. That gives us a sense, does it

not, of the demographics of those people who are online? They have to be able to access the system, do they not?

Commander Steve Head (National Police Co-ordinator for Economic Crime, City of London Police): You are absolutely right. In terms of online crime, there are huge disparities around the country as you go and there are disparities in terms of offenders and in terms of victims and their access to the technology. What we have seen is that quite low-level gangs that previously would have been very much regarded as street gangs have started to touch into some of the economic crimes and minor forms of fraud as a means of raising money for other kinds of criminality as well. It is a global issue. As countries like Brazil and other countries like that go online more and more, you do not necessarily see more victims within those countries but you see more offenders in those countries targeting people in the UK, Europe and the United States.

Jennette Arnold OBE AM: It is very interesting.

Roger Evans AM (Chairman): There is actually quite an interesting map we were supplied with on page 37 of the agenda which shows victims of fraud by ward in Greater London. It seems to show no pattern at all, actually. It is quite difficult to discern something from that.

Jennette Arnold OBE AM: It is interesting, isn't it?

Roger Evans AM (Chairman): OK. Just to return to the outcomes because we are still interested in this, if 5% of the cases had a positive or negative outcome, what has happened to the other 95%? Are they in some sort of limbo?

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): No. Obviously the system that was up and running prior to FALCON being in place meant that investigations took place across the MPS and they had been referred in from Action Fraud. The results of those crimes were not necessarily sent back to Action Fraud and therefore the outcome rate was as low as you see. It is not necessarily the case that nothing happened. It is probably the case that there was an investigation. Our statistician detection rate for last year was approximately 13% but what happened was we were not sending the results back to Action Fraud. There are a number of reasons for that but the basic fact is the officers had to double-key it back to Action Fraud and that just was not happening on a general scale across the MPS. That is now happening because we have put FALCON into place. Two weeks ago, our IT system was actually properly updated and so, when an officer does do that essentially within the MPS, we are then able to return the figures back to Action Fraud. That is the reality around the outcome rate, albeit the 13% certainly is not at the level of positive outcome we would expect in terms of our detections.

Roger Evans AM (Chairman): Raising your outcome rate from 5% to 35% may not be as challenging as it sounds. I suspect it sounds like there is some low-hanging fruit there.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): I do not expect it to be too difficult. The only thing at the moment we are facing is we need to back-record convert a large number for this year alone to try to get to a baseline for next year. In getting that done, my expectation is as long as we are sending back the positive outcomes to Action Fraud, we can at least show where we have actually had some success. The other piece is more administrative and making sure that what is going back is what needs to happen. I am hopeful and optimistic that it will be higher than that, but it depends on some of the back-record conversion issues.

Roger Evans AM (Chairman): This is about better management and clearing a backlog, really.

Detective Superintendent Jayne Snelgrove (Metropolitan Police Service): Yes. Better management of the end to end processes have been discussed and moving forward. We are working with Action Fraud to try to actually join up as much as we can in terms of the IT systems to get this as more of an auto-populated process.

Roger Evans AM (Chairman): All right. Thank you for your answers today. Thank you to Members for their questions. Are there are any other questions Members have? Is there anything that you would like to add? It has been a pretty deeply informed session as usual and very useful. Thank you for your time. We will let you go now.