Online Crime Working Group – 27 November 2014

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

Roger Evans AM (Chairman): Item 5 is today's business, the second evidence session. We have Alex Marshall, the Chief Executive Officer of the College of Policing, who is here to tell us a bit about the specialist training that this work requires. Matthew Allen, the Director of Financial Crime - interesting title - from the British Bankers' Association (BBA), is here to tell us about the approach financial institutions take to online acquisitive crime.

Can I start with you, Mr Marshall? Welcome. Can you tell us about the view of the College of Policing? Do you feel police forces are behind the curve when it comes to tackling cyber-enabled crimes at the moment?

Alex Marshall QPM (Chief Executive Officer, College of Policing): The country, society and policing are to some extent behind the curve on tackling the cyber or online threat. There are lots of very, very good things happening in policing and through the professional body for policing, which is the role of the College of Policing in setting standards and setting out the educational requirement and building the evidence base for police forces in England and Wales. However, it is clear there is an inconsistent response to this threat and that there is much catching-up to be done, not least because a large police workforce that has been very successful in reducing crime over the last ten years, particularly at a time when large cuts have been made, is a workforce where many of them will have been in the police for 15, 20 or 25 years and they are now on a daily basis dealing with complex, online and cyber issues which they were never originally trained for and perhaps would not be their natural leaning.

Roger Evans AM (Chairman): Do chief constables and Police and Crime Commissioners (PCC) share your view about that?

Alex Marshall QPM (Chief Executive Officer, College of Policing): I think they do. There would not be a chief constable and of the 43 there would not be a PCC who does not view this as a serious issue where there is a threat to the people living in their area from online crime. They are all in different ways tackling this threat.

Roger Evans AM (Chairman): Can you tell us a bit about the work that the college is doing to equip forces to deal with this new threat?

Alex Marshall QPM (Chief Executive Officer, College of Policing): Yes. We like to start with the evidence and the research base and we are exploring and have been looking at research and evidence around the cyber threat. It is not as well developed in the evidence base as in other areas of policing. For example, the evidence about what can be achieved with a neighbourhood team is very well developed and it has been tested, peer-reviewed, published and trialled, whereas in this arena the evidence looks less well developed, less well challenged and less well embedded. We set the standards for this area and we will next year be publishing new national standards for online investigation and intelligence. There are some existing standards that we inherited when we came into being 18 months ago and I think they have been caught somewhat in the time they were published around 2010/11.

Then the big push in this area in recent months has been the training that we provide for everyone who works in policing across England and Wales and that is a range of online training - tackling an online threat with online training - and then some specific courses for different skills areas in cyber or online crime and a major programme of cybercrime training that has gone out to every force in the country.

Roger Evans AM (Chairman): Joanne?

Joanne McCartney AM: Yes. I just want to ask some questions on the training, if I may. We noted that a recent Her Majesty's Inspectorate of Constabulary (HMIC) report said that the training offer had very disappointing levels of take-up. As the College of Policing, are you able to enforce training or name-and-shame those forces that do not take it up? What pull do you have?

Alex Marshall QPM (Chief Executive Officer, College of Policing): We are not a regulator. Although we set the standard for policing in all areas - for example, we set standards in tackling child sexual exploitation and we set standards in how to tackle domestic abuse - we do not have an enforcement arm. We set a standard and we take that standard to chief constables for them to implement it in forces and then HMIC then inspects against the standards that we set. Clearly, we do not just set a standard and leave it be. We try to watch what is happening in forces. We also have to understand that the context in different forces can vary and that there will be different local priorities set by the Police and Crime Commissioners.

Joanne McCartney AM: We heard at our last session that online crime spans many different areas now. Is there a case for an element of the training to be in officers' initial training as they join the force?

Alex Marshall QPM (Chief Executive Officer, College of Policing): Yes.

Joanne McCartney AM: Is that something you are looking at?

Alex Marshall QPM (Chief Executive Officer, College of Policing): Absolutely, yes. That is the answer to your question. It is now in their initial training. A fairly large programme we have, which is called the Mainstream Cybercrime Training (MCCT) because in the police we like to reduce everything to a series of letters, is now part of the initial training - what used to be called probationer training - and the development programme for everyone who joins policing. Also, most forces are now putting that in their initial detective training. It is called the Professionalising the Investigation Programme or PIP qualification that detectives do. Therefore, absolutely.

The type of online crime that officers will deal with ranges from everything they used to deal with from antisocial behaviour through to the most serious crimes and there is now an online aspect to pretty much all of those. Even if you took a straightforward fight outside a pub, which unfortunately still occasionally happens, there would have been a time when two or three people might have seen it and you would have had someone with injuries and someone accused of punching someone else. Now it may well be that the pictures have been circulated, it has appeared on Facebook, three people have tweeted it and two people have filmed it on their mobile phones while it was going on. Even a straightforward assault outside a pub is likely to have quite a large online context to it.

Joanne McCartney AM: We visited Action Fraud yesterday and one of the things they told us was that they do some sifting and if a certain report meets a threshold, they will then pass it on to local police to investigate. They said that these were ones that they believed were solvable and so they were solvable crimes. From where you stand, having a broad view of the different forces, is the solvability dependent on the training that officers have had in those different forces?

Alex Marshall QPM (Chief Executive Officer, College of Policing): In my understanding of how Action Fraud makes that decision, it is not based at all on the take-up of training in different forces. By the way, I was not disputing --

Joanne McCartney AM: No, I think it was the outcome. Action Fraud said they send it out believing it is solvable. However, when it hits different forces, it just strikes me that if they have not had the training and if they do not have the skilled officers, irrespective of whether a crime is solvable or not, it may not be solved.

Alex Marshall QPM (Chief Executive Officer, College of Policing): Yes. The HMIC report you referenced I do not dispute at all. There is inconsistency in the way the training is being taken up and in some cases there is clearly a need to accelerate that for that individual force and for that chief constable. Yes, it is quite clear that there will be forces with more people who are trained in this area and they have more people skilled and dedicated to this type of work.

Of course, the chief constables are making the operational decisions locally and have to prioritise where they place their detectives and their other investigators and it has to be in line with the priorities set by the Police and Crime Commissioners in their annual plans. You will see different priorities in different forces and this priority will feature in a different position in different forces.

Roger Evans AM (Chairman): Just on that, are you satisfied with the Metropolitan Police Service's (MPS) take-up of the training that you offer?

Alex Marshall QPM (Chief Executive Officer, College of Policing): From looking at the MPS approach to this, it is quite clear that from the top, both from the Mayor's Office and from the Commissioner, from what they have declared publicly and committed to tackle in this arena, there is absolutely leadership about this being a priority and they clearly take it very seriously. The MPS - and I very much approve of the approach they are taking - have set up a team of specialists to deal with particular aspects of business crime and fraud and online fraud, while they are also trying to raise the skill levels of everyone else who works in the MPS who will come across that pub fight or will come across another allegation of online crime. In essence, the MPS's approach, which is to have a department with specialists and to dedicate resources to it and then try to raise the skill levels elsewhere, is a very good model. I know the MPS, the same as everyone else, is still catching up in terms of equipping everyone on the front line to have those skills.

Roger Evans AM (Chairman): Does that model contain an inherent weakness in that the department of specialists, the Falcon Command, could become siloed and separated from the rest of the force?

Alex Marshall QPM (Chief Executive Officer, College of Policing): Absolutely. That is a risk and it always is when you employ a team of specialists. If you took domestic abuse, it would be the same. Where is the handover between the first response and the specialism? What are the out-of-hours arrangements? How do you make sure that the level that that team accepts is the right level? Those risks are always there. It is then for the organisation to make sure its people are well informed about how they operate within the specialist team and outside the specialist team.

I have no day-to-day knowledge of how Operation Falcon works, but I have seen its setup and I have seen its objectives. It looks like a very strong approach to me.

Roger Evans AM (Chairman): All right. That is reassuring. What do you feel are the challenges that Falcon is going to be facing in the future?

Alex Marshall QPM (Chief Executive Officer, College of Policing): Volume and remit because, as more and more types of offending develop an online and arguably a cyber aspect, depending what definition we would put on the term 'cyber' in that context, then they are likely to have to constantly make decisions about what is within their responsibility and what remains outside. The same with every other aspect of policing, the very first response is often the most important one. If that then triggers the right secondary and tertiary actions, including by a specialist department, then that works really well. If the very initial decision goes in the wrong direction, it is hard them for members of the public or the citizens or the residents of London to feel that they have had a really good service.

Roger Evans AM (Chairman): OK. How do you feel we should measure the performance of Falcon once it has been set up? This should not just be about catching criminals. There is a prevention aspect here as well, is there not?

Alex Marshall QPM (Chief Executive Officer, College of Policing): The whole ethos of the College of Policing starts with prevention and so we are the 'what works' centre for preventing crime in the way that the National Institute for Health and Care Excellence (NICE) is the 'what works' centre for health, early years foundation, et cetera. Prevention seems to be the long-term best and most valuable approach we can take in this arena. Working with industry, working with businesses and working with individual people across London and across the country and getting that message of education and prevention out, both in terms of people's actions and in changing of systems and products, would appear to be where success lies. In terms of how you assess the performance, I am afraid that is not an arena I can help with.

Roger Evans AM (Chairman): All right. It is just that we are going to be talking to them about the way they set their objectives later on. Perhaps some input from you would give us some additional ideas about how we can task them on it.

Alex Marshall QPM (Chief Executive Officer, College of Policing): Perhaps the only way I can really help is to say that the approach the College of Policing is taking to this is to start with what the evidence is. What have we established? What do we clearly know about the problem that we are facing? What standards have been set for people to operate to? What have we done to make sure that people have the skill levels to operate? That is in my own context.

Roger Evans AM (Chairman): Thank you.

Tony Arbour AM: As a rider to the great challenges, is one of the things about the skills related to work in Falcon the fact that it is a uniquely marketable skill, whereas most policing skills are not - how shall I put it - in great shortage as far as the wider world is concerned? Therefore, is one of the problems going to be that, firstly, Falcon will have difficulty recruiting people who are able to do the job and, secondly, when you have them there is a risk that they will be poached, which does not happen in other areas of policing?

Alex Marshall QPM (Chief Executive Officer, College of Policing): I can remember working somewhere where some of the police cars were Jaguars and all the mechanics were trained up to be Jaguar mechanics. Funnily enough, they had a better offer from Jaguar to work on the cars there than they did to work in the police workshop, many years ago.

There is that risk and one of the areas the college is looking into at the moment is the type of people we recruit into policing and what the skills are that we should be looking for in the next generation of police officers and police staff. I do not think it is the case that we have been recruiting people that necessarily we

can say have the skills that would help us tackle this problem. Therefore, we have a responsibility as the College of Policing to look at the people who are coming into policing at the beginning.

There are a lot of very good, clever and successful investigators and detectives in policing, some of whom will go into this world. Yes, once they are trained in this arena, they probably are more marketable, particularly in the London context compared to other parts of the country. That is an ongoing risk and the City of London Police faces that risk as well with the number of people they have who are specialists in dealing with fraud. There is always the risk that they could be an attractive candidate for a bank. However, in policing we have to be more accepting that people may move in and out of a police career and not just come in and stay for 35 or 40 years in the way that they used to. We should not feel threatened by it. As those people leave, we should be able to attract other good people in who already have some of those skills.

Tony Arbour AM: I am pleased to hear that, but is the real problem not related so much to you having them and them being poached but actually recruiting people in the first place who are able instantly to deal with these characters? I assume that - how shall I put it nicely - someone who is innumerate and illiterate is unlikely to perpetrate fraud. Therefore, to combat these people, we need people who are infinitely more numerate and more literate in the cyber world than the people who are committing the crime. How do you recruit such people? They are unlikely to come through the normal Winsor [Review] recruitment process, are they not?

Alex Marshall QPM (Chief Executive Officer, College of Policing): Within policing anyway, there will be people who are very skilled in this area and naturally will move to that part of the business. Many forces have specialist teams already dealing with online investigation in the same way they have specialists dealing with other areas and they are people who have joined in the normal recruiting and have then specialised. Absolutely, this is an area where the police will also have to attract people in who are specialists. The National Crime Agency has exactly the same challenge bringing people in who have these skills. It is a competitive market, particularly in London, and it will be hard to bring in particularly more senior experienced people in this arena.

However, I do not want to write off the next generation of people applying to join the police, many of whom are likely to have very high degrees of skills in using technology. They operate online constantly as 22-year-olds living in London now in whatever job they are already in. Therefore, I am quite optimistic that the next generation will come in with a relatively higher level of skills perhaps than those of us who joined in 1980 with regard to technology.

Jennette Arnold OBE AM: Just going back to when you were talking about the College of Policing preparing officers to deal with this, you said quite interesting things about the prevention strand of this. Yesterday we were very enthused by what we heard from the leading officers at the City of London Police because they clearly were working and tackling it along the three lines of the Peel principles. I just wondered. Should you not be doing the same? This is more than prevention. Do you not need special investigative skills and should you not be looking at that? I cannot think what the third principle is. It is prevent, disrupt and then enforce.

Alex Marshall QPM (Chief Executive Officer, College of Policing): Yes.

Jennette Arnold OBE AM: Therefore, for instance, I was expecting you to be talking about, if you like, a wider network of thinking between you and other colleges of policing around the world. I am not really excited about what I have heard you say. Put it like that. As a victim and other victims, I am not excited. There has to be more from the College of Policing to try to get our officers ahead. Or is it the case that, coming from the profession, practice will always be in front of the academic thinking?

Alex Marshall QPM (Chief Executive Officer, College of Policing): In terms of understanding the latest approaches, we work with universities, we work with other police forces, we study the research there is in this area. What I have not done yet is tell you the different types of training that we provide to forces and I did not want to just provide a list --

Jennette Arnold OBE AM: I am too impatient.

Alex Marshall QPM (Chief Executive Officer, College of Policing): -- but clearly in not doing so I have left a gap that has left you disappointed. Included in our training is how to deal with all the communications data that is inherent in cybercrime, how to do cyber investigations and investigate crime on the internet, the first response to dealing with cybercrime, cybercrime and digital policing introduction, cybercrime and digital policing investigation, digital communications on social media, and cybercrime and policing. Then we do an accreditation so that officers can qualify in communications data investigator. There is then a higher level 1 for their managers. There is communications data analysis. Then we get into the MCCT. That is about how you investigate online crime, how you prevent it, how you pursue the perpetrator, how you chase the money, how you use the communications equipment, how you make a basic analysis of the phone data and the computer data, when you should send these pieces of equipment off for specialist analysis --

Jennette Arnold OBE AM: I am excited! It is OK.

Alex Marshall QPM (Chief Executive Officer, College of Policing): I did not just want to give you a long list. My point is that we provide a huge range of online and face-to-face training course to equip people to do it.

However, my earlier point was that different forces will be in different places in terms of how many people have done that training and how ready the force is to deal with all those aspects of it. They will all have some specialists, but they will all have people on the front end who might have to deal with this at any moment now.

Jennette Arnold OBE AM: Thank you.

Roger Evans AM (Chairman): Thank you. That was useful. We will move on to questions to the banking sector.

Caroline Pidgeon MBE AM (Deputy Chair): I just will pick up one thing with Alex first and then I will come to Matthew [Allen]. You did not actually answer Roger's question when he asked what the training take-up had been from the MPS for your programme. Are you able to give us any further details on that and how they compare?

Alex Marshall QPM (Chief Executive Officer, College of Policing): I do not have the MPS take-up. What I can say is that in the MCCT that is for most people, we are aiming to train 3,000 people nationally by the end of this financial year. I checked the October figures, the last full month, and we had trained 300 people in October.

The reason I do not have a breakdown of all the different figures is that we make the package available and it is a matter for the force locally whether they put that as a one-off course for their people to do in their first two years when they are becoming investigators or whether they put parts of it across the whole of the two years. It is quite hard to say that 26 have done it here and 30 have done it there.

I will try to deal with this quickly. I know you have other questions you need to ask. For example, in the first two years of officers' training, which is when they complete all their initial training, they will deal with issues such as theft, domestic abuse, fraud or whatever it might be. Some forces choose to put the cyber online bit against each of those subjects as they go through them. Some do the whole cyber element as a big chunk of the two years. It makes getting the data back on who is now currently trained, who is half-trained and who has only just started being trained almost impossible.

However, I did check October and we had 300 people complete the course. We think it will be 3,000 nationally by the end of the financial year. I do not have the MPS figures to hand. I am sorry.

Caroline Pidgeon MBE AM (Deputy Chair): OK. It will come up later in the second half of today, but some of these very specialist skills that are needed are really techie stuff way beyond me and most of us here. Would it not actually be better to have some police staff trained to do that rather than it actually being police officers? It seems to me there is a real balance in this, more than perhaps in any other area, and you need people with that computer specialism who may not want to just be police officers and who want to specialise in that computer world.

Alex Marshall QPM (Chief Executive Officer, College of Policing): My own experience as a chief constable in a force near London is that we employed lots of police staff, not police officers, in the roles of financial investigator, fraud and in particular doing the work on - what is the right term - our economic crime units and looking at the content of computers, phones and other devices. That is not a skill you would normally find in a police officer and so we employed people separately.

The challenge for the police service is that you can bring those people in directly to do that one post. We need to make that part of a career structure so that policing is much more open to people coming in with those skills to work within policing and they are likely to come and go. That is not our traditional model and it is the responsibility of the College to change the nature of the way we recruit and retain people in policing.

However, you are absolutely right. You can employ people who are not police officers and the National Crime Agency does exactly that.

Caroline Pidgeon MBE AM (Deputy Chair): Yes, brilliant. Thank you for that. Matthew, I have some questions for you. Thank you so much for coming along this morning. Perhaps you could open with - from your experience and your organisation's experience - the scale of online fraud and theft in London, if you can give us that specifically.

Matthew Allen (Director, Financial Crime, British Bankers' Association): Thank you and, firstly, thank you to the Chairman and the Committee for the opportunity to speak today. The banking industry is trying to explain as clearly and as transparently as possible the approach we are taking and so we are grateful.

This is a difficult question you have given me first up. I do not think we know the scale of online fraud. I share the views of Donald Toon, the Director of the Economic Crime Command of the National Crime Agency, who said we simply do not fully understand the extent of the challenge here. To break that down, there are statistics that show a piece of the picture. It is important to recognise that online fraud or cybercrime - the terms are used interchangeably - covers a vast array of criminal offending, as my colleague from the College of Policing described.

There are online offences that affect retail banking customers, for example. There is also online offending targeted at banks rather than the customer, et cetera. Most financial crimes have an online element now.

There are of course other types of criminal offending which are targeted attacks against banks for other purposes and which I do not think this Committee is looking at, but it is worth having that context because we as banks have to consider all of those risks. There are other factors as well that need to be considered. The economic factors have a significant impact on the risks posed. There is evidence that criminals have targeted the financially vulnerable over recent years. Geopolitical events can radically alter the risk profile certainly to banks.

I probably have not answered your question directly, but it is important to recognise that simply stating a figure is not really going to give you the full picture. Also, just to add, the challenge your Committee will have is determining London versus the national and international challenge. We set out very clearly in our evidence to the Home Affairs Select Committee that this is no longer a London issue or a United Kingdom (UK) issue. This is a global issue. Certainly for the banking industry, given that most of our 230 members operate across the world, we do not look at this as a London issue or as a UK issue. We are looking at this as an international issue.

Caroline Pidgeon MBE AM (Deputy Chair): I appreciate that and, as I say, from our site visit yesterday it clearly is international in nature. However, in evidence to the Home Affairs Committee back in 2012, the cost for the UK banking sector was estimated to be £475 million for online crime. Is that a figure you recognise?

Matthew Allen (Director, Financial Crime, British Bankers' Association): I recognise that figure, but I do not think it is the full picture. It is for online crime against retail banks. That is my understanding of the figure. That is not the full picture. We represent private banks, corporate banks and investment banks. There are other factors that need to be considered.

It is also worth saying that I think that was the losses from online crime. There are other residual factors that need to be taken into account: the resources that are needed to respond, the wider impacts on reputation, et cetera. That is a figure and it is one of the figures, but it is not the full story.

Caroline Pidgeon MBE AM (Deputy Chair): Yes. I realise that this is incredibly complex and that I am trying to look at it at quite a simple level.

In terms of retail banking and the banks that we would all use, is there just huge under-recording of any credit card or other fraud? If I am a victim and someone has somehow used my card online and I then contact the bank, they will refund me the money. Therefore, from my point of view, it is annoying and I have to wait for a new card, but it has been refunded and you have resolved it for me and thank you very much. However, I do not report that anywhere. Most people do not report that anywhere. Is there not an issue that lots of these crimes are not being reported anywhere and we do not have a true picture?

Matthew Allen (Director, Financial Crime, British Bankers' Association): You are quite correct that most victims of fraud who are retail banking customers are refunded. The most recent industry estimate was 98%. There is a question around whether that is a good figure or not. Customers who are victims of fraud are encouraged to report to Action Fraud.

Caroline Pidgeon MBE AM (Deputy Chair): Is that proactively done now by banks? If it is reported, do they automatically --

Matthew Allen (Director, Financial Crime, British Bankers' Association): Yes, in a number of ways. Individual banks provide advice. At an industry level, we put out a public communication last month in partnership with the City of London Police, the Financial Conduct Authority and others in which we very

explicitly said, "We encourage reporting to Action Fraud". Of course, then you will have the figures going up and that is one of the challenges with getting to the heart of the reality of the problem we face in terms of online offending. Increased reporting does paint a worse picture, in a sense, but a more accurate picture is important. Therefore, victims are encouraged to report and there is more reporting. Whether that is the total volume of fraud that is actually occurring I doubt, but we are proactively encouraging reporting.

Caroline Pidgeon MBE AM (Deputy Chair): OK. There is an issue between how you treat individuals - whom you refund very quickly and who have a very good service - and small businesses that are victims of online crime. Often, they are not refunded in the same way. Why do you treat individuals and small businesses so differently?

Matthew Allen (Director, Financial Crime, British Bankers' Association): There are legal obligations in relation to refunding customers that are set out at a European level. There is a challenge in terms of refunds, actually. To properly analyse financial crime cases, which are often very complex, requires some investigation. There are also requirements on banks to refund promptly and to process transactions quickly and there is a tension there.

In terms of small businesses, as I understand it, there will be contractual arrangements between the small business and the bank. We are engaging through Government departments and directly with some business organisations on this issue. However, the requirements for individual customers, as I understand it, are set out in European law.

Caroline Pidgeon MBE AM (Deputy Chair): I understand that it is particularly small businesses that have lost money through online fraud, especially if it is down to what is classed by the bank as a 'customer error' and you just do not refund it. We have had that in some evidence that came before us. Is there a thing that banks are not prioritising tackling online fraud against businesses in the same way?

Matthew Allen (Director, Financial Crime, British Bankers' Association): No, I do not think that is the case. Part of the approach we are taking is to promote and strengthen standards in our clients and we are working closely with a number of Government departments on that issue to try to help small businesses to understand approaches that can be taken.

In relation to the specific issue of cases of small and medium-sized enterprises (SMEs) not being refunded, I would need to go away and do some further research. We would be happy to write if that would be helpful.

Caroline Pidgeon MBE AM (Deputy Chair): If you could, that would be. We have had that in evidence from Cifas. Is that how they pronounce it? Yes.

Matthew Allen (Director, Financial Crime, British Bankers' Association): If I could just add, we work very closely with Cifas and they are closer to the practical fraud prevention work and so they may be better placed. We will talk to them. Our job is to support banks across the full range of financial crime and security threats they face and we have 230 banks. I think the Cifas membership is smaller and they may be better placed to give you details, but we will write back to you.

Caroline Pidgeon MBE AM (Deputy Chair): That would be helpful. How do banks work with the police forces across the country? How do you work closely with the police?

Matthew Allen (Director, Financial Crime, British Bankers' Association): We have an excellent relationship with the police. Individual banks work very closely with a number of police forces. As the BBA, we

have proactively attempted to facilitate a stronger dialogue between the banking industry - and I mean the banking industry in its broadest sense, particularly smaller firms that have had less interaction in the past with law enforcement.

We do that through a number of channels. We sit on a range of Government committees including the Association of Chief Police Officers (ACPO) Economic Crime Committee. We also run operational groups with the City of London Police and the National Crime Agency, which are our main partners. That allows banks to sit in a room with law enforcement and to really look at the operational challenges, whether the processes are working, what new trends we are seeing, etc.

We also run a system with the National Crime Agency and the City of London Police at present that allows those forces to send information directly to banks through an online portal. These are alerts and assessments. That has worked very well. The City of London Police process with us has saved over £100 million in terms of losses prevented. In January next year, we are starting the rollout of a new alert service that will allow 12 public bodies to send this information through a single system. The point of this is to make sure banks have a coherent mechanism to receive this information. That allows them to take quicker actions, both in terms of individual accounts and also in terms of strategy-setting. If they understand how the criminal methodologies are changing, they can better target their resources. Therefore, we have an excellent relationship particularly with the City of London Police and the National Crime Agency. We will be meeting Falcon next week and we are looking forward to that.

I would, though, add that the challenges to our members are not UK challenges. Most of the problems are international and that is where there is a particular issue around a co-ordinated international law enforcement response to tackle what are very sophisticated and well-resourced criminal networks. They are the groups that are doing the harm. Europol and Interpol have a very important role in that respect. The banking industry has signed a memorandum of understanding with Europol, which is a great step, but there is a lot more to do and we are very committed to that piece.

Caroline Pidgeon MBE AM (Deputy Chair): It sounds like you have a very good approach to this. Are there any areas that could be strengthened to make this approach even more effective?

Matthew Allen (Director, Financial Crime, British Bankers' Association): I have some sympathy for the comments around capability. This is challenging. The way that financial crime has evolved - including fraud - means that people who deal with this on a day-to-day basis need to have a new range of skills. Within banks, you need to have information technology (IT) expertise. You need to have investigation expertise. You also need to understand the vast array of laws that we have to comply with, notably data protection, payments processing and financial inclusion laws. The data protection piece is a particularly challenging area.

Within the banking industry, there is work underway to build capabilities. We need to work with law enforcement to help law enforcement to build their skills and experience. We have started a programme of providing briefings by banks to law enforcement and 25 City of London Police officers came over and talked to us about banking to understand how banking works and how that could affect their jobs. We have had similar events with the National Crime Agency where we have had bankers talking to law enforcement.

There is a lot more we can do in terms of understanding our respective agendas and the challenges as well as building our collective skills and capabilities. That will be critical.

Caroline Pidgeon MBE AM (Deputy Chair): A greater understanding of the industries and how they work, as it were, would help?

Matthew Allen (Director, Financial Crime, British Bankers' Association): Yes. There has been a lot of progress. There is a better understanding of law enforcement drivers now within the banking industry. Law enforcement has a better understanding of bank drivers, which can be different. However, we have a collective interest in building our skills and capabilities to address very sophisticated criminal networks and we are committed to that.

Caroline Pidgeon MBE AM (Deputy Chair): Do you agree with the UK Fraud Prevention Service that private organisations such as banks might need to be compelled to share their fraud data with the police to help them tackle online crime?

Matthew Allen (Director, Financial Crime, British Bankers' Association): I was interested in that set of comments. There is a genuine debate at the moment about information-sharing and we as the BBA on behalf of our members are working very closely with the Government departments on this. This is difficult.

I do think there is a case for reviewing whether the legislative framework in this area is up to date with current threats. The criminal offending has changed radically and laws need to keep up. However, there is a genuine tension between sharing information with law enforcement for the purposes of preventing crime and respecting other very important legal obligations and rights such as data protection and privacy. Post-Snowden [Edward Snowden, US computer analyst and whistle-blower], certainly in Europe, that discussion has become more prominent and it is finding the right balance.

What is a more helpful way of describing it is to allow banks a safe legal route to provide information to law enforcement. I am not sure compulsion is necessarily the approach I would recommend, but certainly we are interested in modifications to the law to allow safe information sharing.

Caroline Pidgeon MBE AM (Deputy Chair): Is there too much, as it were, competition between the banks? Is fraud seen as a competitive area and actually at one level do banks not want to reveal their weaknesses, as it were, or how much they may have lost or whatever to competitors? Is that a problem within the industry? When you have these meetings - and I know you represent everybody - is that pushed aside and everyone just says, "We have had this", "We are talking about that", and so on?

Matthew Allen (Director, Financial Crime, British Bankers' Association): At a general level, no. We run seven committees. Banks are very open with each other. They recognise that actually it is in their interests to help other banks to have strong controls because a successful attack against one bank can affect other banks. Therefore, at a general level, no.

There are difficulties depending on the type of fraud we are talking about. For retail banking fraud, it is slightly easier. When we are talking about fraud in the corporate investment banking space, there are other sensitivities we have to consider and we are working more closely with investment and corporate banks and with private banks, actually. However, there are challenges in that area, particularly for a global bank that may be headquartered in another jurisdiction that has a slightly different approach to laws.

To give an example, one of our member banks identified a fraud in a European country that was affecting its London branch. It took a fair amount of time to work out whether that information could be shared from one European Union (EU) country with London. By the time that legal process had been gone through, it was basically too late. Therefore, there are wider legal challenges as well. However, I do not think this is on a general level seen as a competitive issue.

Caroline Pidgeon MBE AM (Deputy Chair): It is just about getting the right framework or whatever so that you can share these things legally?

Matthew Allen (Director, Financial Crime, British Bankers' Association): Yes, and so that banks can share known fraud data with each other. It is the suspicion of financial crime that is the key at an earlier stage and that is more difficult.

Caroline Pidgeon MBE AM (Deputy Chair): Thank you.

Tony Arbour AM: Really, it is in relation to that. It is easy to understand how it could be in the interests of your members not to report crime and indeed not to even talk to other banks simply because of loss of reputation. Am I misjudging you in thinking that preservation of their reputation is an important factor as far as your members are concerned?

Matthew Allen (Director, Financial Crime, British Bankers' Association): It is very important to say firstly that there are regulatory obligations on reporting financial crime. Banks report around 250 suspicious activity reports to the National Crime Agency of financial crime. There is a separate reporting line to Action Fraud which covers financial crime. As I understand it, roughly 80% of those reports will have a fraud dimension. There is a reporting line there. Then there is the vast amount of information that is given to police forces, including by banks reporting through Action Fraud as well. Therefore, there is significant reporting of financial crime, including fraud.

What is a challenge is the complexity of some of these cases. In many cases, you actually need to understand banking. I am not from a banking background. I have been in the industry only three years. My eyes have been opened to the challenge in understanding some of these very complex cases we deal with. It is less a challenge of reporting; it is getting those cases through the system. Commander Head [National Police Co-ordinator for Economic Crime, City of London Corporation] will be better placed to talk about that throughput.

Tony Arbour AM: Let me give you an example. Supposing a sophisticated fraudster discovers a failure in the main computer system of the bank and carries out some sort of theft because they have discovered this failure in the system. It would be easy to understand that the bank would not want to make this public and therefore anybody who had been caught out by this would be refunded. You have already told us how punctual the banks are to deal with this matter. The reason that they would deal with the matter so rapidly and not report it is because the reputational loss might be much greater in fact if it got out that there was a failure in the system.

Matthew Allen (Director, Financial Crime, British Bankers' Association): If I may, there is a difference between reporting to public authorities and reporting publicly. There are mechanisms for banks to report incidents. There is also a separate system for reporting attacks that may have a systemic impact. There are various reporting mechanisms. Banks will not necessarily be reporting publicly at that stage and I accept that, but there are very good reasons for that. There are very clear reporting mechanisms, there are regulatory obligations and there are legal obligations for reporting to public authorities. Care has to be taken in terms of publicising that an incident has happened and there are mechanisms in place for that where banks work with the public authorities on the appropriate time to announce a major attack if that is what (overspeaking)

Tony Arbour AM: It is interesting that you talk about that because it appears - and we have discussed this before in relation to other police matters - that certain crimes are reporting as being 'non-crimes'. That sort of sounds like what you are describing. If the bank's system has been hacked, it will not tell the public and it may be that it will not tell anyone else either and therefore it is a 'non-crime'.

Matthew Allen (Director, Financial Crime, British Bankers' Association): I am not an expert on the classification of reports and when they become 'crimes'. That is a police matter. What I am saying is that there are mechanisms for banks to provide information to public authorities. We are very diligent in meeting those legal and regulatory obligations. A vast amount of information is provided to the public authorities.

I think the scenario you are talking about is a targeted attack on a bank, which may be for different purposes other than fraud. There are arrangements in place for that. There have been tests in the City with the regulators of how the system is arranged. There is a report of those scenario tests and the recommendations are worked on. I am not an expert on the 'non-crime' piece. Police colleagues will be better placed for that.

Tony Arbour AM: Can I ask Mr Marshall? I am right, am I not, that the largest area of 'non-crimes' relates to this area of criminality when an offence is 'non-crimed'?

Alex Marshall QPM (Chief Executive Officer, College of Policing): For something to be 'no-crimed' or 'non-crimed', it would have been recorded in the first place with the incoming call in the command-and-control system if it is reported to a police force and then, as a result of an initial investigation, it would have to be established that no crime had happened for it to then be declared as a 'no-crime'. That is quite different from when a crime is recorded and then an initial investigation is carried out and it is decided either to refer it to another agency or not to carry out any further secondary or tertiary investigation. That would not be a 'no-crime'. It would be recorded as a crime but the investigation has finished at a particular point.

However, the issue of what the banks know from the attacks that might happen upon them and how that is then reported to the police and how that appears in the overall crime figures is a very, very good question. The banks have their considerations, but the police are in the position that if they do not know about the attacks, they definitely cannot do anything about them and they cannot record them. Therefore, the idea about sharing information and being clear on what the law allows to happen and what is right for the citizen and for people to know what is happening is still a perfectly valid question.

Tony Arbour AM: You have really touched on the reason why we are having this investigation: part of our normal work is to do with the general level of crime. If these crimes are not reported, then the general level of crime seems much lower than it really is.

Matthew Allen (Director, Financial Crime, British Bankers' Association): If I may, I would not want to give the impression that banks are not reporting crimes where they are legally required to. There is significant report. I am saying there are a number of mechanisms. Action Fraud is not the sole mechanism in this area. There are other mechanisms.

There is also a question, of course. If so much information is provided which is very relevant and very helpful, the extent to which those cases can be acted on is of course an important element as well. In the banking industry, we have created lots of information-gathering systems and lots of systems for recording information. It is what you do with that information that is also important. When you are dealing with cases that are global in nature and very complex, there are real challenges in responding to that vast amount of information. That is the challenge for law enforcement.

Tony Arbour AM: Thank you, Chairman.

Roger Evans AM (Chairman): All right. Thank you. This is a complex issue and so we appreciate you giving us your time this morning to help the Committee to understand it. Are there any other questions from

Members before we complete this session? No. Is there anything that either of you feel we have missed or would like to add? No.

Alex Marshall QPM (Chief Executive Officer, College of Policing): Thank you.

Matthew Allen (Director, Financial Crime, British Bankers' Association): Thanks.

Roger Evans AM (Chairman): That is good. That is reassuring. Thank you for your time.