Online Crime Working Group – 21 October 2014

Transcript of Item 5 – Online Crime

Roger Evans AM (Chairman): Welcome to our witnesses. Professor Marian Fitzgerald is on her way, delayed by the storm no doubt. However, here with us we have Professor Mark Button from the University of Portsmouth, the Director of the Centre for Counter Fraud Studies. Simon Dukes is the Chief Executive Officer of CIFAS, the United Kingdom's (UK) fraud prevention service. Welcome to you both.

We have a few questions for you this morning and really what we are aiming to do is to take evidence about the scope of the problem and the police response to it. Can I start, Mr Dukes, with you just to ask how the internet is changing the way that criminals operate?

Simon Dukes (Chief Executive Officer, CIFAS): From the wider sense and also what we have seen, the National Crime Agency has written very well about this idea of cyber-enabled and cyber-dependent type crimes. Cyber-dependent stuff and the real technical denial-of-service attacks are not something that my organisation looks at. However, cyber-enabled crime, the use of the internet in order to speed up and commit fraud - in the case of CIFAS and what we look at - at greater pace and at greater scale, is absolutely evident.

Therefore, yes, it has certainly increased the speed. Of course the fact that technology changes as such a rate as well means that you are running to catch up sometimes when trying to prevent some of these crimes.

Roger Evans AM (Chairman): Professor Button, do you have anything to add?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Yes, particularly if you look at the mass-marketing type frauds, what the internet and the changes in technology have enabled is the industrialisation of these scams.

Think about the traditional '419' letters. Traditionally, they were sent through the mail. You needed to spend money to buy the paper and buy the postage. Now all you need to do is sit at a computer anywhere in the world to have the ability to send out large numbers of emails and you can reach huge numbers of individuals. With advertising services and products online, previously you were required to go to magazines, newspapers, etc, to try and advertise services. Now all you need to do is put up a website.

Therefore, we have seen a situation where particularly mass-marketing frauds have been able to be industrialised on a large scale, enabling lots of individuals to commit those crimes not in small numbers but in very large numbers. That, combined with the easy access everyone has now in this country to the internet, mobile phones and to those types of technology, makes it a much higher risk to everybody.

Roger Evans AM (Chairman): What do we know about the sorts of people who commit these crimes? Are they already criminals or are they a new breed?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): This is always the million-dollar question. Unfortunately, there has not been a huge amount of research on the types of individuals that commit this type of crime. First of all, there is an element that comes from overseas, a lot of African countries and Eastern Europe, but we also have a home-grown problem as well.

If you look anecdotally through the media, the people who do actually get caught are a mix of what I would see as traditional criminals as well as new types of individuals who maybe see the easy lure of lots of money and commit a crime that way. Only last week, some of our students from Portsmouth University were convicted of a romance scam. They did this scam while they were students. I think there is obviously an organised crime element, but it is also a wider element as well. It is clearly an area we need to do more research on to uncover more about the types of people who get involved in these things.

Roger Evans AM (Chairman): You said "lots of money". Is this a very profitable area for criminals?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): In the scam that I just mentioned, I think they netted several hundred thousand pounds. Therefore, it can be very lucrative, yes.

Roger Evans AM (Chairman): Yes. Why is the internet an attractive option for criminals rather than the traditional crimes we have come to know?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): First of all, it is very easy to do it on a large scale. You can sit in a room and send out emails. You can sit in a room and set up a website. It is relatively easy to do. You can reach a large group of individuals. We have all gained from accessing certain types of services and meeting certain types of people that would be much more difficult to do prior to the internet. That has provided, also, opportunities for people to link into particular groups of individuals.

If you take a very common scam, a holiday scam, all someone has to do is put up a website with pictures of a nice holiday destination and make it look quite official and put in a reasonable price. That attracts some individuals to buy bogus holidays. It is the ease. It is the industrialisation.

The other thing when you think about it is that it is fraud at a distance. You are not having to look someone in the eye and do something horrible to them. You have the anonymity of the internet to hide behind.

Simon Dukes (Chief Executive Officer, CIFAS): Can I add that I absolutely agree with everything Mark [Button] said? Also, you do not need to be a geek to be able to do this. The technology is available and you can purchase it and use it. There are even websites to show you how to use it. Therefore, it is very accessible to everyone.

Roger Evans AM (Chairman): I know that with the evidence that you have presented to us you have given us a breakdown of the number of offences that occur in London. Is that unusually high compared to other places? Is there a particular risk for Londoners here?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think because of the high population here, of course there is going to be a higher number. However, what we have seen through research we have done and looking at the data we have is that, unlike perhaps some of the other types of more traditional crimes, cybercrime can happen anywhere and everywhere. There is no particular grouping.

Just purely out of interest - and my apologies that I did not have time to do anything more sophisticated - just within a kilometre of this building, these are the red dots of cyber-fraud that we have seen happen in the last few months. It is interesting to see that it is --

Roger Evans AM (Chairman): Would we be able to have a copy of that?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I will certainly get you a copy of that, yes, absolutely.

Caroline Pidgeon MBE AM: It is frightening, is it not?

Roger Evans AM (Chairman): I note that some of the dots are bigger than others.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): The larger dots equate to larger numbers of victims.

Roger Evans AM (Chairman): They are not the size of the fraud; they are the number of victims in a particular location?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): The number of victims, yes.

Roger Evans AM (Chairman): Yes. Is that typical of London or is it going to be worse in a location like this?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): There will be some areas perhaps which have a higher victim rate, but it is pretty constant across the capital.

Caroline Pidgeon MBE AM: Can I just ask what might sound a really stupid question? I understand people setting up these websites and, as you say, the holiday one is a good example. How do they get mass numbers of emails? That is what I do not understand. I can understand if I have a website and there is an email there and presumably there is technology that can - I do not know - collect all of those. But how do you get an ordinary person's private email? How do they get those to then be able to send this direct marketing? I am always suspicious of anything, but if you see something from what might be your bank, some people might be fooled into clicking on links and so on.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Certainly, first of all, just like any business, you can buy lists of emails. If you are setting up a legitimate holiday website company, you could buy that kind of information. Therefore, that is one step.

A lot of them also have the ability to generate emails. You get large organisations with common emails and they have software which can generate that kind of thing. You will see a lot of organisations have filters that can filter that kind of spam out.

There are also illicit lists that some of the fraudsters actually trade with one another. They have lists of individuals who have already fallen for a scam and they trade that kind of information. Those are just some of the ways they can get that kind of information.

Caroline Pidgeon MBE AM: Is it the same with credit card numbers? You hear of these scams where something is done at a cash register, but I do not understand again, particularly as credit card companies more and more have three digits on the back now and, depending on your company, when you try to buy something online you then have to go in with another password or whatever. How do they get those numbers and how do they work if they would not have that sort of password?

Simon Dukes (Chief Executive Officer, CIFAS): I have two things, really, to add to what Mark [Button] said. The first is that this is where perhaps this type of crime differs from more traditional crimes in that data has a value wherever that data has come from, whether it is bought and sold on the dark web by criminals or whether it is actually obtained by insiders in an organisation because they realise it is not just access to petty cash or invoicing that is going to provide them with money. They can take the customer or client list from an organisation or they can take the staff list from an organisation and that itself has value to criminals precisely for that reason.

These can be coupled with other datasets. Do not forget we cannot look at these in isolation. It might be that they have credit card numbers. It might be that they have names. They might have addresses. It is putting all this information together in order to make something that is actually useable either by themselves in order to carry out a fraud or a scam or a crime or indeed to sell on to other criminals.

The term that is often used is 'social engineering'. Actually, in some cases we have seen, with just a name and a telephone number, the criminal does the rest. They phone up the person and they use various techniques to elicit information in order to improve and enrich the data they have on that individual. They might then use it themselves or they might sell it on. As Mark [Button] said earlier, it is an industrial type scam.

Caroline Pidgeon MBE AM: Thank you.

Roger Evans AM (Chairman): Interesting.

Joanne McCartney AM: Yes. I want to look at the size of the problem that we have. We have had some warnings recently. For example, Bernard Hogan-Howe [Commissioner of Police of the Metropolis] has said that nearly 4 million frauds of credit cards or electronic frauds he knows have not been reported or included in the crime statistics. We have had the Home Affairs Select Committee last year referring to a 'black hole' that enables lots of these crimes to go not only undetected but under-reported as well.

What do you think is the scale and why are they not included in the national statistics?

Simon Dukes (Chief Executive Officer, CIFAS): They do not include them. Certainly, looking purely from my perspective as head of CIFAS, of course we are looking at fraud in particular, whether it is cyber-fraud or traditional fraud, and we are seeing probably 1,000 new frauds every day. All of those are reported to law enforcement.

Joanne McCartney AM: Those are the ones that are reported to you every day?

Simon Dukes (Chief Executive Officer, CIFAS): Those are the ones that are reported by the membership of CIFAS to us every day which then go on to law enforcement. However, they are not included in the official crime statistics, as you quite rightly say and as has been said before. My understanding is that if you added those types of crimes to the crime statistics, you would get quite a significant rise. Professor Fitzgerald is far more knowledgeable about this particular issue than I am. In 2013 there were about 7.5 million crimes reported. It would probably rise to about 11 million crimes reported. It is a significant increase if you add fraud.

Why is it not being reported? There are a number of reasons. Sometimes it is not seen as a crime necessarily or perhaps as a victimless crime by some people. Perhaps there is embarrassment in reporting the type of cybercrime that Mark [Button] referred to earlier, the dating scam. The Financial Conduct Authority produced a very interesting piece of research last week which said that victims of a particular type of boiler-room scam - that is a share-dealing scam - were on average about 55 years old plus, perhaps had a bit of experience in

share-dealing before, had some spare cash at hand and actually felt really embarrassed about having been scammed in that way. On the whole, many of them did not report it. Therefore, there is a sense of embarrassment.

There is a sense of, "Where is the victim? Who is the victim?" Banks, building societies and others of course are reimbursing citizens at least if they lose money --

Joanne McCartney AM: Citizens, if they get paid, do not probably report it, yes?

Simon Dukes (Chief Executive Officer, CIFAS): If you lose from your bank account some money, often the banks are reimbursing that sum or your credit card if your credit card has been skimmed.

It adds to the idea that perhaps we are not taking fraud seriously in the way that we should. It is a bit like going out today along the street and dropping litter because you know that the street-sweeper is going to be along in half an hour and will clear it all up for you. It is that sort of responsibility aspect, which perhaps we will come on to, but I am very interested in the citizens taking responsibility more for their own cybersecurity.

Joanne McCartney AM: You said 1,000 frauds a day are reported to you?

Simon Dukes (Chief Executive Officer, CIFAS): Yes.

Joanne McCartney AM: Do you know how many are not reported to you? Do you have any idea of what percentage does get reported to you? No?

Simon Dukes (Chief Executive Officer, CIFAS): I am afraid not, no.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): The other thing we need to consider is that if you look at the most accurate measure of crime, it is the England and Wales Crime Survey. We do not ask the question in that survey, other than, "Have you been a victim of plastic-card fraud in the last 12 months?" There are lots of other types of frauds that potentially a person has been a victim of and which they do not even get the opportunity to raise in that crime survey.

The other thing is, as Simon [Dukes] pointed out, that a lot of these frauds are very embarrassing. The way the England and Wales Crime Survey is undertaken is through interviews. You can imagine that sort of gentleman in the share-dealing scam or someone who had been in a romance scam having an interviewer coming to the door, "Have you been a victim of this type of crime?" It is going to be embarrassing for a lot of people. We need to find new ways of measuring the size of the problem.

Having said that, if we look at some of the other countries and some smaller-scale prevalence work that has been undertaken in this country, some of it is a bit dated but the Office of Fair Trading did a prevalence survey back in 2006 on mass-marketing fraud and 8% had been a victim. Now equate that across the whole of the UK and millions of victims would be added to those crime figures.

Joanne McCartney AM: When you say 80 million had been a -- did you say 80 million?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): It was 8%.

Joanne McCartney AM: Are they people who have clicked back and responded as opposed to just received the information?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): These are people who have actually lost some money. Obviously, you also have to remember in 2006 that the internet was not as prevalent as it is today. Most people did not have mobile phones with the internet. The opportunities for that type of fraud to occur have increased substantially.

Joanne McCartney AM: OK. Has any research been done in other countries to measure the scale of the problem that you are aware of, or not?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Yes. In America and Australia, they have done more advanced prevalence surveys. For instance, in Australia, there was a study in 2010/11 and 6.7% of the population aged over 15 were the victim of at least one personal fraud in the past 12 months. In America, you have the Federal Trade Commission, which has done various studies related to this. In 2005, 13.5% had been the victim of a consumer fraud.

Obviously, the internet has moved on since a lot of those studies have been undertaken and the risk is probably much higher now. It does highlight the need for more of this kind of research to try to find out what the true extent of the problem is.

Joanne McCartney AM: OK. Is there any reason to think that we are not similar to Australia or America in the extent of the problem?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): They are obviously very similar English language-speaking countries. Possibly there might be some differences if you went to Western Europe because of the kinds of challenges for, say, someone in Africa committing a fraud against someone who speaks German. There might be some reductions there. However, when we are talking about Australia, America and Canada, it is a similar kind of base.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): I am very sorry. I do apologise for being late.

There is also evidence that, relative to other countries in Europe, we actually use the internet far more for online shopping. In terms of vulnerability, that gives you a sense of the scale relative to other countries in Europe.

Joanne McCartney AM: We were just looking at what the size of the problem is and perhaps, Professor Fitzgerald, I can ask you about crime statistics. We have heard that they underestimate the amount of online crime. I wonder if you had anything to add to that. Also, how can the difficulties of measuring online crime be overcome? We have heard about the British Crime Survey.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): The challenges have been overstated and they come from confusion between the fact that the police-recorded statistics and the crime survey capture different things and they both have their limitations. They have been set up as though they were alternative measures of a definitive notion of crime. The police only know the crimes that get reported to them and the crimes the police themselves cover, which of course increasingly in this context could be enormous. The MPS has always lagged behind on its detection rates, but if it cracks a major case with thousands and thousands of victims, its detection rate would go from very low to over 100% if it is measured against the crimes that get reported to it. That is something that needs to be looked at. The idea

that we are fixated on detections only in relation to crimes that have been reported to the police really is called into question when we are looking at an area like this.

However, when you look at the crime survey, it is effectively a misnomer. It does not measure crime. It measures the experience of victimisation of individuals aged over 16 who are living in private households. If you take burglary, for example, it will capture the burglaries that those people have experienced which have not been reported to the police, but in fact the police statistics show that non-domestic burglaries are now running at twice the rate of domestic burglaries. The police are capturing a much wider range of criminality - albeit with limitations - than the crime survey and the crime survey is covering the experience of victimisation.

That being so, I think one of the problems we face at the moment is that the public's experience of victimisation has changed tremendously since the early or mid-1990s and the crime survey has failed to keep up with that. It simply is not representing the experience of private individuals living in private households, aged over 16, of victimisation because more and more of what they are experiencing will be happening online. Partly as a result of that, it has shown remarkable falls in crime consistently since 1997, falls which have now become so remarkable that they are being called into question. The latest fall is a miraculous 16%, which, given that the police figures have been hung out to dry and have had the National Statistics Kitemark taken away from them, is somewhat ironic since the most the police ever managed for all their gaming was 9%. What it is omitting in terms of ordinary, everyday people's experience is the central issue here. You can throw all sorts of things into it about how many victims there were and whether they were really the bank or the individual or whatever. What that victim has experienced is what we want to know from the crime survey and we have increasingly lost track of it.

I know that the Office of National Statistics (ONS) has now said that it is testing questions about this, the results of which will not be available, oddly, until October 2015, well after the next general election. When it did ask a question about card fraud very belatedly in 2005, of course, it discovered that it was happening at such a scale that had it been included in its estimate of the true level of crime, that estimate would have looked rather different. Indeed, an estimate that it did finally come out with in July, which it has now revised downwards, showed that it would actually have increased the crime survey's estimate of crime by 50%. However, amongst arguments which year after year it refined about why it did not include it in its estimate of crime was that actually maybe it was not the individual who was the victim but it was the commercial organisation. That says it all because you are not capturing the totality of crime if you are only capturing that narrow range which happens to adults in private households.

The odd thing is that it has actually been asking questions on this subject for at least the last three years. Although it has changed some of the questions and certainly expanded them, it has consistently asked one question for three years in a row in one of the follow-ups to the main survey. That was a question which includes whether within the last 12 months the respondent has experienced, while they were using the internet, loss of money, unauthorised access to or use of personal data - for example, email account or bank account - and abusive or threatening behaviour. That information has been sitting there and even if the numbers were relatively small, if you aggregated the three years, you would at least get a very good sense, I think, of the extent to which those same individuals were experiencing these crimes online relative to their responses to the standard questions.

Even when the Select Committee did its report last July on e-crime - and I have looked at the Home Office submission to it and also the Government response - I do not think any mention was made at that time to the Select Committee, which surely would have wanted to know this, that these questions were even being asked.

Joanne McCartney AM: Is the data available?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): It is there. However, it was only by virtue of someone who was looking into these issues alerting me to the fact that the questionnaires were online and that if I looked at them I would find that these questions had been there. I was gobsmacked because never in defending the absence of information on cyber-enabled crime has the ONS said, "Yes, we are sitting on this data". I am sure, as I say, that the Select Committee would have welcomed some sort of steer, which would surely have been available, even rough-and-ready.

Joanne McCartney AM: The data has not been released, though? Although now the question has been asked, the data has not been released?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): No. There has been no great play made of the fact that the questions were being asked. Only now when they are saying that they are testing these new questions, the results of which will not be available until after the next general election, do they say that they have been doing some experimenting but it was only very rough-and-ready and nothing definitive has come out of it. However, if you have had that same question asked three years in a row, there is something there.

Joanne McCartney AM: The ONS has said before that some of the challenges around it were the difficulty in identifying who was the actual victim, which we have picked up --

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): It is if the victim believes they are a victim and this is a victimisation survey.

Joanne McCartney AM: -- and, if it is mass marketing, how many victims you should actually count. Is it everyone who received an email or is it only those who responded? Then, where is the offence originating from?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): That is an issue for the police to deal with in terms of how they count crime and how they count detections. In terms of what the survey is supposed to capture, which is the experience of this narrow range of individuals in this country of victimisation, it is a large and growing part of it and we have not been capturing it. Those objections do not obtain.

Joanne McCartney AM: OK.

Roger Evans AM (Chairman): Surely the police and the people who collect statistics have already been through that process when you consider people doing a similar thing with direct mail campaigns. They are exactly the same challenges.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): The problem with this area of course is, in so far as these figures are dependent on people reporting, we have the whole issue here of whether people report and whether they are less likely to report and, if so, whether they know who to report to.

Do not forget that since 2007 any victim of card fraud or fraud of any kind is not supposed, as they would if they were a victim of burglary or theft or whatever, to go to the local police. If they go to the local police, they find that the police are not interested. That is partly because the police have been given a dispensation that they can keep these off their books, thank goodness, since they are under the cosh to endlessly keep crime figures looking as though they are going down and have been caught out in the ways in which they did that. However, these offences were to be reported to something called Action Fraud, which most victims, I suspect,

would never have heard of. First of all there are a lot of inhibitors to people reporting these sorts of crimes anyway and we can maybe go into that later, but insofar as they do, they go to the first normal port of call and find that they are not interested.

The chances of the extent being captured given the normal problems of poor reporting and so on will be even more so in this case. It will not be down to the police. It will be down to Action Fraud and the City of London Police, who then are supposed to pass on a very small amount of the reports they get back to the local police, who of course have no ownership of the problem and have enough on their plates in the first place. The chances of victims getting satisfaction, even in that knowledge that someone was not done for their crime but someone was done for a lot of other crimes probably including theirs, are so remote that I cannot see why most victims would be motivated to-- Unlike with card fraud, of course, with the other types of fraud, they cannot expect any recompense.

Joanne McCartney AM: Can I ask Simon what evidence there is to suggest that online crimes are occurring on a large scale? I suppose by that I mean some of the data we may have heard about and I find the 1,000 a day shocking. Also, do you have any evidence? Are these organised criminal networks as opposed to individuals just taking a chance in their own living rooms on things? What is the evidence?

Simon Dukes (Chief Executive Officer, CIFAS): From the data that we have, I cannot really answer the last bit of that question because, as I said, the crimes - the frauds, in our case - are passed to the police and it is for them then, of course, as Professor Fitzgerald has said, to package them up and to push them out to the force where probably the victim is based.

What I would say is that of the 1,000 frauds a day that are reported to us, about 65% of those are committed online. Of those, over 80% are what we would call identification crimes, where individuals' identities are stolen either in order to carry out an application-type fraud to get goods or credit in somebody else's name or indeed to actually hijack somebody else's bank account or credit card account and using it. That we see certainly on the increase proportionately to the other types of fraud that are reported to us.

Joanne McCartney AM: What role do other bodies have in this? I am thinking about banks and mobile phone companies. What role do they have in collecting data and passing it on to you or the police or elsewhere? Is there an incentive within their organisations not to report?

Simon Dukes (Chief Executive Officer, CIFAS): If you will just forgive me a second and indulge me, 26 years ago CIFAS was formed on Oxford Street precisely because a number of retailers were fed up with criminal gangs going around and using credit cards with the same MO *[modus operandi]* and the same people. Because it was high volume and low value, relatively speaking, the police were just not equipped to deal with it. It was the suggestion of the police, actually, who said, "If you get together and share information on individuals or the card numbers or the types of scam, then one of you might get hit but it will prevent everyone else getting hit with the same scam". This is how this data-sharing, in a very basic way in those days on the telephone or through a fax, started. Fast forward 26 years and we now share millions of pieces of data in real time between 320 or so organisations, but the basic theory still is there. If somebody gets hit by a fraud or a scam and if they share that data with everyone else, then everyone stands a better chance of protecting themselves.

What we are seeing is that 40% of the benefit that one company will get out of using CIFAS comes from a scam that has hit outside its sector. The banks get benefit from sharing data with the insurance companies, who get benefit from sharing data with the telecommunication companies , with the asset finance guys and with the public sector. They all share data in one big pot and that is how they protect themselves and reduce fraud risk, basically. That is what it comes down to. Your question was about the role that bodies have.

Joanne McCartney AM: What role they have, yes.

Simon Dukes (Chief Executive Officer, CIFAS): From my perspective, there is a real need to share data on fraud and online crime because, that way, we stand a better chance of protecting ourselves. Criminals are doing it all the time without international boundaries and without data-sharing agreement issues. They are buying and selling credit card details and names of potential victims all the time.

Joanne McCartney AM: Yes. In fact, in your written response to us, something stood out for me. You said, "Criminals work better together than industry".

Simon Dukes (Chief Executive Officer, CIFAS): I fear that that is sometimes true, yes.

Joanne McCartney AM: Yes. The second part of that, then, is that we have heard there might be a perverse incentive to under-report as well for these companies and we had the recent debacle with eBay not letting its customers know that their account details and passwords had been hacked and emails not going out to alert people. Is that an issue?

Simon Dukes (Chief Executive Officer, CIFAS): Colleagues here will perhaps have better sight of it. I think we are looking at two slightly different things. The crimes that are reported to an organisation like mine are reported in order to protect other organisations. Therefore, there is an incentive to report crimes in that way. What you are talking about is data loss of perhaps clients or customers and there , of course, is a reputational hit to the company concerned about not only the amount of data being lost but also of course what subsequently might happen in terms of regulatory comeback and legal costs.

Joanne McCartney AM: I will pursue that in a second, if I can. When Sir Bernard [Hogan-Howe, Commissioner of Police of the Metropolis] talked recently about the under-reporting of the issue, he also actually pointed the finger at the banks and credit card companies whom he said did not want to reveal how much they lost to criminals because it would reveal how vulnerable they were.

Simon Dukes (Chief Executive Officer, CIFAS): Yes. I think there is a sense of that, certainly.

Joanne McCartney AM: There is a sense of that?

Simon Dukes (Chief Executive Officer, CIFAS): Yes. However, what we have tried to do over the last 25 years is to make fraud non-competitive. The fact is that if you are a bank and you share data on a crime with us and another organisation will see it, it will know that you have suffered that crime. The whole benefit comes from not acknowledging that and not trying to gain competitive advantage from that but actually using that to reduce fraud risk overall.

Of course, there will be banks that are constantly trying to improve their cybersecurity online, especially with mobile applications now as well, and would not necessarily want to release information that might be of advantage to competitors or, indeed, if citizens might think, "It is safer to go with Bank A than it is with Bank B and I am going to go with Bank A".

Joanne McCartney AM: From your experience, if a bank or a credit card company does realise that there is an issue or that there is some fraud happening, will it always alert victims or will it try not to?

Simon Dukes (Chief Executive Officer, CIFAS): From my experience, it will, yes.

Joanne McCartney AM: OK. I do not know if Professors Button or Fitzgerald have any comments on those last two points about an incentive perhaps not to report. I used the eBay example.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Certainly I hear anecdotal evidence from some of the fraud investigators that I talk to that there is often an interesting debate over whether it is a bad debt or a fraud. It is always very interesting when you look at a lot of the companies what is the level of bad debt and fraud and to look at those figures rather than just fraud.

The other point I would make is that we do have to distinguish between the frauds which are involving the banking institutions or financial institutions where there is obviously an incentive for those companies to deal with them and to have some kind of response and the mass-marketing type frauds where it is just the fraudsters against the victims and where there is no incentive to go to anybody to secure your money back because it is not going to happen.

Joanne McCartney AM: One of you mentioned earlier the 'dark web' and about how information is shared or whatever. How difficult is that to detect?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I do not have a huge amount of expertise and experience of this, but I had a colleague who had expertise in this and he showed me some of the trading rooms on the dark net where you could buy credit card details. They were being sold in batches and you could buy for $30 five credit card numbers which you could obviously then use for whatever fraudulent purpose you wanted. There is a whole set of those types of websites out there, but it is not something I know a great deal about.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): From a slightly different perspective, it was ever thus about commercial organisations not wanting to reveal stuff which would spoil their reputations before we ever reached this era and passing on losses to customers in terms of increased prices and so on. It has always been like that. This, in that sense, is no different.

I do think, though, what we need to take seriously - and going back to what I said about the crime survey and the police both having limitations but capturing different things and how they should have been somehow complementary - is that we are never going to get a definitive measure of what crime is going on. However, I suspect, increasingly, that with all of these diverse methods of committing crime and diverse organisations to which people may report - internet service providers, mobile phone companies and so on - there is an increasing need to try to get a best-possible estimate of crime and to be able to track that honestly without political interference by capturing all of the possible sources and treating them as complementary. There will be overlap, but if you try to get a best estimate which will bring in however much all of those organisations are prepared to admit to, as long as the amount they admit to remains constant over time, you can then start to track trends. That pooling in terms of getting an overview of how much crime is happening and looking at the policing, detection and investigation end is going to be important.

A separate issue is people's experience of victimisation. That comes through the crime survey, which performs a different role and which I have already talked about, where there are not the same sorts of obstacles as are being put forward.

Tony Arbour AM: You talked about the data-sharing between the banks and so on and they can inform each other and learn from each other's mistakes. How invulnerable, in fact, is that shared data? We have heard already that those people who have once been subjected to fraud are likely to be susceptible again. All this data-sharing that you have about these people is an absolute goldmine. How invulnerable are you?

Simon Dukes (Chief Executive Officer, CIFAS): Clearly, I am not going to answer that question because --

Tony Arbour AM: Are you invulnerable?

Simon Dukes (Chief Executive Officer, CIFAS): -- the type of criminals and the type of world that we are living in is that, if anyone says they are invulnerable, you can bet your life the next day --

Tony Arbour AM: It is a challenge?

Simon Dukes (Chief Executive Officer, CIFAS): It is challenge and everyone will have a pop at you. All I can say is that we go through a rigorous Government approved and ISO [International Organization for Standardization] approved process in order to make sure that we come up to good - very good, in fact - cybersecurity standards. However, yes, you are right. It is the way that data, of course, as well, is not just put into one big pot. It is the way you keep it and separate it that also adds to the security.

Caroline Pidgeon MBE AM: I wanted to move on to the challenging of policing online crime. We seem to be quoting Bernard Hogan-Howe [Commissioner of Police of the Metropolis] a lot, but he has talked about this huge emerging challenge and how the police have not got to grips with it at all, really, to date.

How well do you really think the internet is currently policed?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): If I can slightly rephrase that to how well fraud is policed, obviously the internet being part of that, the police are behind the curve. We have had all these changes over the last 10 to 15 years with the internet and huge opportunities for new frauds to take place. However, the resources and the infrastructure, which have always been poor for fraud, just simply have not kept up to date.

Recently, we did freedom of information requests of every police force in the UK. When you take out financial investigators and you have just the police officers and the fraud investigators, there are around about 650. These are specially trained officers. Of course, police forces will always say that other police officers will deal with frauds, but the reality is that for most police officers frauds are pretty low on their list of priorities. It is not the sexy kind of crime that most of them have an interest or a desire to be investigating.

Therefore, just simply in terms of the resources and the infrastructure, the police in general are behind the curve on this.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): I do not think there has been any incentive for them to get ahead of the curve, either, given the pressure to endlessly show crime going down. This is going to open a whole big can of worms. Besides that, with diminishing resources, "How could we possibly stretch ourselves further" I think has been the attitude.

That said, I know it is now proposed that there should be specially trained officers and so on. If we look at the lower-level end of cyber-enabled crime now being perpetrated by the usual suspects but along with a lot of other crimes as well, it is all part of the mix because these young people are the PlayStation and Xbox generation and they may be functionally illiterate but they have grown up with those skills and they can do it. As the research done by McGuire and co[1] for the Home Office showed - unlike what Yar[2] was saying in 2006 where you would have to have specialist skills to be able to do this and you would have to be pretty bright and

[1] Mike McGuire and Samantha Dowling, *Cyber Crime: A Review of the Evidence*, 2013
[2] Majid Yar, *Cybercrime and Society, 2006*

middle class and so on - everyone now has access to the Internet. The packages are there. You need no more skill than to be able to log on.

If you move to the police side and the people who are saying that we need to specially train people certainly for dealing with that level of stuff, it is not true because a lot of officers are also of the Xbox and PlayStation generation. They have those skills and for a lot of them it is sitting there within their own ranks and a lot of them would give their eyeteeth to have a pop at this. At the same time, you have to remember that if they are dealing with the usual suspects locally, they are going to be dealing with them increasingly with one hand tied behind their backs if they do not know about this whole other area that those same people are now getting into as well and some of the scams that they are pulling in real space.

I was just looking the other day for some other work that I was doing on stop-and-search and I was looking at people who had been searched repeatedly. I went to the arrest data to see whether the same people had been arrested at all over the previous year. What really struck me was that most of them had but, where they had been arrested numerous times, just the mix of offences that they were being arrested for. These people are not going to be specialists. They are going to be doing low-level online stuff and they are going to be doing it at a low level. For the local police, they actually need to deal with that.

The other thing that I would say is about creaming it off to a specialist department. Yes, you will need special expertise for dealing with the higher level, more organised stuff and so on. However, for the everyday stuff, which I think is what concerns us, and in the everyday experience of ordinary Londoners, it is only going to get dealt with by the regular police you would normally report to. They just need to be aware of what the usual suspects are up to. Just hiving off this area to somebody else is utterly artificial and perverse.

Caroline Pidgeon MBE AM: Simon, do you agree with that? Obviously, the College of Policing has set up this new framework and police forces can assess how well they are doing. Her Majesty's Inspectorate of Constabulary (HMIC) has reported that take-up of training has been poor. However, according to Marion [Fitzgerald] here, we do not need that because a lot of the lower level ordinary officers would be able to deal with it.

Simon Dukes (Chief Executive Officer, CIFAS): It is a prioritisation and resource issue, to be honest. You look at the MPS and you think of the incredible range of crimes that it has to deal with from international organised criminal gangs through to the opportunist thief, trafficking people, domestic violence and child abuse. It is a massive thing. Then you have to put fraud and cybercrime into that mix as well and it is a huge resource and prioritisation headache for the Chief Commissioner.

I am somewhere in between, I guess, the two Professors here because we probably do need a bit of specialisation perhaps when it comes to some of the evidence-gathering for some of these cybercrimes, which can be slightly different. Good, solid, investigative, dogged determination and skill-set are probably as relevant as they are in traditional crimes.

What I would say is that what Professor Fitzgerald said about the mix of crime and the mix of offences goes on to something that I just mentioned earlier. You do not get criminals specialising in credit card crime or insurance scams. They will do a whole range, which goes back to my thing about how sharing data on different types of crime certainly does help.

The final point, really, is going on to your question about how the internet is currently policed. That is really quite interesting because I said at the start about citizens having to take some responsibility as well. I do think that just as when we left to come here today we made sure that our house or our flat was well secured, the windows closed, the doors locked - and you might have an alarm - and whatever it might be, we have to take

similar sorts of precautions online. The difference is that equally, just as when you leave your house and walk to the Tube station, you do not expect to be mugged and you expect some sort of security on the streets, we need to have something which helps in terms of online security in cyberspace as well.

I am encouraged by all the work that is being done with Cyber Streetwise and the Cyber-security Information Sharing Partnership and the work for businesses and all this sort of thing is great. However, you do wonder whether this multitude of advice and guidance can sometimes be a little bit confusing for people. Citizens have to take some responsibility, too.

Caroline Pidgeon MBE AM: What do you make of the MPS's decision to launch this new central command? It has 300 police officers and staff. Do you welcome that and think they will be able to do some of this more specialist work or do you think it is just not enough at all to deal with this whole area?

Simon Dukes (Chief Executive Officer, CIFAS): I do not know about the numbers, but I certainly welcome the initiative. The MPS has a good history of work in this area, the Police Central e-Crime Unit, a couple of years ago. Certainly I have worked with them in the past. Having a fraud and crime online specialism is absolutely a good thing and we certainly support it.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): In a sense it is related to that, but it needs to be a resource for everyone else as well. There is a danger of us conceiving of this as a different and new crime. It is not. It is a dimension of crime and an increasing dimension of crime at every level: serious, organised, international crime and low-level stuff committed by the usual suspects whose dads would have been out burgling 30 years ago. Unless we start understanding it like that, it is a bit like talking about knife crime when actually 'knife crime' as such does not exist. It is whether a certain offence was perpetrated with the threat or the use of a knife, but the substantive offence is the substantive offence. We are talking about the same here and there is a danger that we are talking about it as something separate.

Therefore, since it goes across the piece, everyone across the piece who is dealing with the whole range of crimes needs to be able to engage with this increasing dimension of those crimes. Having a specialist unit can do certain things and maybe where real specialist skills are needed intensively for certain types of investigation, but unless that resource is made available and the existing potential unleashed across all of those other areas, we really are going to miss out very badly except for in those high-profile specialist crimes which that unit will deal with.

There is always this danger of salami-slicing or hiving things off and the people who are dealing with the everyday stuff do not feel any ownership or responsibility and yet it is increasingly part of the victim experience for the people whose crime reports they are taking.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): You have to remember police culture. For a lot of police officers, these types of crimes are just not something they have an interest in dealing with. It is a very, very low priority. A lot of cybercrimes will come in and will immediately be put at the bottom of their list. If you leave it to the general police, unless you find a way to really change police culture to embrace that, I do not think you are going to get the attention --

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): We are talking about fraud in a very narrow, technical, traditional sense. What I think we are talking about here in terms of victims' experience is scams and ordinary people with whom a lot of police officers would feel a lot of sympathy, like an old lady who is a victim of some confidence trickster. They would feel a lot of sympathy when somebody has actually been quite innocently scammed out of a whole load of money, has lost a holiday of a lifetime and this sort of thing. I do think that of ordinary police officers because there is this distinction

between 'deserving victims' and 'underserving' victims which is very much part of police culture as well. Quite a lot of the people they encounter here they would see as deserving victims of scams rather than of fraud in the highly technical financial - "We do not understand this stuff" - area that they do not like to deal with.

Caroline Pidgeon MBE AM: That is very interesting. Did you want to perhaps --

Tony Arbour AM: Marian, you have several times talked about "the usual suspects". You are simply saying this is a 21st century crime as opposed to a 19th century crime when they could go out and see the victim. Is that actually true given that so much of what we have been told already suggests that this is an international crime? We surely did not get that in the early part of the 20th century or in the early days of policing? They would be your local usual suspects.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): That is what I am talking about. There is a whole spectrum here and at one end of the spectrum you will have the usual suspects. At the other end of the spectrum you have the potential for a lot more international stuff than was possible a century ago.

However, there is evidence that not much has been done. There was a lovely study by someone called James Treadwell[3] *F* who did interviews with young men who had been dealing in counterfeit goods. He had some wonderful quotes about how when you are dealing off the back of a lorry or at a car boot sale or whatever you can get caught by the 'Old Bill', but online it is easy. Nobody cares. They are all talking about how much easier it is to do the same stuff - offload counterfeit goods or whatever - online than it was when they stood the physical risk of being caught. Of course, they can do it on a much larger scale and so on. That is what is happening. It is borne out by the work that was done by McGuire and co[4] for the Home Office last October.

The other thing that intrigues me though is that as well as the usual suspects, we have these high-profile cases of hackers with Asperger's Syndrome and all the rest of it, very middle class, very bright young men and so on. Beyond that, again for the Xbox and PlayStation generation, in the same way that people who would not have been seen in the past in the newsagents buying stuff off the top shelf can now experience all sorts of things in the privacy of their own room without a member of the church actually seeing them at it, you also have people who are very canny at using the internet. For young people, it is classic within criminology that the peak age of offending is 17 and that age range is notoriously attracted by risk and excitement and does not yet have a mature full grasp of the likely consequences. It was there writ large in the riots and so on. There is the buzz and the carnival of crime. If you have someone who spends an awful lot of time on the internet and who suddenly realises that if they pit their skills they could actually invade someone's privacy, pit themselves against security advisers and so on. It may actually be pulling in a much wider range of people than the usual suspects because of the excitement and the buzz. The only extreme examples we know of this are hackers who have broken into the Pentagon and so on, but that is the far end of a spectrum.

David Wall's work[5] [has an interview with a young man who said that some friends showed him what they were doing and said there was no risk to it. He tried it and it worked and there was the excitement of discovering that. However, he said if he had had to face the victim face-to-face, "no way". There is something about the anonymity and so on which also will attract people.

The police officers that I talk to actually started getting into this without any specialist skills but were trying to track down what was happening to stolen goods which had been reported to the police. They ended up

[3] F*rom the Car Boot to Booting It Up? EBay, Online Counterfeit Crime and the Transformation of the Criminal Marketplace*, 2012
[4] Mike McGuire and Samantha Dowling, *Cyber Crime: A Review of the Evidence*
[5] *Cybercrime: The Transformation of Crime in the Information Age*, 2007

looking online at far more stolen goods than they could ever give back because a lot of them had never been reported stolen in the first place. They 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.

Tony Arbour AM: On your point about the usual suspects, the usual suspects in this particular kind of crime are a much smaller proportion of the perpetrators, if you like, than of traditional crime?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): Possibly. We do not know. It really is an area which is worth exploring.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): One thing I can also highlight to you with regards to the number of frauds that come from overseas is that there has been no research done that I am aware of in this country but there has been a lot on the extent of fraud coming from beyond the United States of America (USA). There is a body called the Internet Crime Complaint Centre and about a quarter of its complaints come from overseas. It gives an overview from an American perspective of how big it might be in this country and in terms of where these frauds are coming from.

Caroline Pidgeon MBE AM: I wanted to pick up that, as you have been saying, this is such a complex area and we are dealing so much with the unknown today and how we actually try to solve some of these crimes.

Where should police really be focusing their resources? Should they be focusing on high-value online crimes against businesses rather than those against individuals? Where is the right place for them to focus resources? Simon, do you want to kick off?

Simon Dukes (Chief Executive Officer, CIFAS): I do think it will depend, really, on the type of crime. The difficulty, I suppose, here has already been alluded to. Because of the nature of the internet and because it is such an incredible enabler for, for example, the 419 type of fraud --

Caroline Pidgeon MBE AM: What do you mean by "419"? It was mentioned earlier.

Simon Dukes (Chief Executive Officer, CIFAS): The classic one perhaps - although most of them come from the USA now, I believe - would come from Africa and it would be that a person has access to a lot of money but there is an obstacle in the way and it needs perhaps a little bung just to set up an account or, "Can we use your account to put the money through? We will leave some money for you". There are many, many different variations. Of course, it ultimately ends up in the victim paying the fraudster money in order to somehow release these funds, which of course never existed in the first place. It is a classic scam that has been going on for many, many decades. I am sure colleagues here will know far more about the history of it than I do.

However, the fact is that, as Mark [Button] said earlier, in order to carry out that type of scam years ago it had to be a letter and it had to be posted and there was some sort of investment in the materials needed in order to carry it out. Now it can be carried out at a massive scale. I do not know what the percentage is but presumably 100,000 or so of these are sent out. The fraudster only needs one and the costs are well and truly covered. You can imagine putting out millions and millions of them.

The reason I was saying that is that there is a sense of scale. It might be one fraudster. It might actually be only one victim. However, the attempted crimes are hundreds of thousands, perhaps millions. There is, therefore, a bit of thought needed on behalf of law enforcement as to where and how they are going to put

their resources in order for the greatest impact. I absolutely do not know the answer to that, but certainly the scale of what we are seeing is 1,000 frauds a day reported to us. Do not forget that we are only one vehicle for reporting fraud to the City of London Police. You have Action Fraud. You have colleagues in Financial Fraud Action UK and there will be other ways that industry at least is reporting frauds to the police. That makes up the totality of the hundreds of thousands of frauds that we see every year.

Caroline Pidgeon MBE AM: Should they just focus on these very high-value crimes because it is all too difficult?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): First of all, I would hope they do not just concentrate purely upon individual victims. There is a large group of small and medium enterprises (SMEs) and small businesses that often get missed out in this picture. The large companies generally have their own infrastructure to protect themselves and they can normally look after themselves and put together the information and evidence to pass to the police. I would hope that it is a focus on the individuals and those smaller businesses.

Perhaps a more important question is not just to focus on investigation because it is very resource intensive. Even with the large numbers that this organisation is going to have, there is only going to be a limited number of actual investigations that are going to be successful each year. I would hope that they do a lot more in terms of disruption. There are lots of activities they could do to make it more difficult for fraudsters to operate, closing down websites and those types of things that make it more difficult for fraudsters actually to operate, as well as engaging much more in prevention.

We have the National Fraud Authority, which was leading on those types of issues. The Government has decided to get rid of the National Fraud Authority and those preventative functions have fallen to the Home Office, but I have not seen a great deal that the Home Office has been doing since it has taken over those responsibilities. In essence, a lot of these preventative functions are going to be left to the police and other organisations that have an interest in this area. I would hope that they use their resources in a wide range of those different areas that I have just mentioned and do not just focus on the small number of investigations which are high-value.

Caroline Pidgeon MBE AM: Marian, what do you think?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): In terms of specialist resources, there is no easy answer and I do take your point about SMEs and small businesses. They are often the ones who really lose out in all of this.

However, I would say what we have to look at is two things. It is where you focus your specialist resources and also - I keep banging on about this - from my perspective it is in terms of the ordinary, everyday Londoners who are victims of this sort of offence. We have to make sure that this dimension is integrated into the work of all police officers dealing with the public and their everyday experience of crime because this is a large and increasing part of it. There are those two aspects and we must not lose sight of that second aspect. This has to be a dimension of all routine police work dealing with members of the public in the low-level stuff. You will need specialist resources for the high-level stuff and then there are hard choices to be made about where to focus that. However, we should not do that at the expense of this very, very wide range of ordinary people's experiences which is increasingly perpetrated in this way.

Simon Dukes (Chief Executive Officer, CIFAS): Can I just add to that?

Caroline Pidgeon MBE AM: Yes, sure.

Simon Dukes (Chief Executive Officer, CIFAS): I absolutely underline the SME point and in particular, unlike with citizens, banks of course are not refunding SMEs for money lost through online fraud, especially if it is down to what they class as 'customer error'. If you have an employee working in the company thinking that they are being helpful and perhaps clicking on an email that they should not and they enter bank details and all of a sudden the money is gone, the banks are not refunding that. The SMEs are getting hit and a six-figure sum coming out of an SME could be absolutely fatal.

That is why certainly we support the Mayor's Office for Policing and Crime's initiative on digital security, which I know is being worked on at the moment. It is an excellent way of plugging into and hopefully uplifting the online security awareness of SMEs in the capital.

Joanne McCartney AM: Simon, your written response to us talks about cases that have gone through the National Fraud Intelligence Bureau, which I believe is run by the City of London Police.

Simon Dukes (Chief Executive Officer, CIFAS): Yes.

Joanne McCartney AM: It says that resources - which I am assuming are policing resources - are almost exclusively allocated to reviewing the large and growing number of Action Fraud reports from individual financial victims. You go on to say that although there were 81,000 reports of financial fraud against public and private organisations, only 589 of those reports were sent to the MPS for investigation. I am just wondering why such a small amount actually get sent to the police in the first place.

Simon Dukes (Chief Executive Officer, CIFAS): It really is dependent on the resource available and of course the evidence available to put them into an investigable package, if you like. There might be a fraud that has been reported, but if the evidence is not there to take it forward, it is very difficult to --

Joanne McCartney AM: For cases that go through Action Fraud, before you pass them to the police, do you have to have a certain evidential package there to pass on to the police or is it not for the police to then act on every single report they get?

Simon Dukes (Chief Executive Officer, CIFAS): Action Fraud is run by the City of London Police and it is a separate system whereby it is a vehicle for public citizens to report, as Professor Fitzgerald was saying, scams in particular because the type of frauds that you get against plastic cards or bank accounts are usually not reported to Action Fraud. Sometimes they are, but usually it is the bank reporting them to CIFAS and then CIFAS then reporting them straight on to the police. It is a dual channel, really.

Joanne McCartney AM: On that disparity between the 81,000 and the 500-odd that were sent for investigation, those 81,000 are actually handled by the City of London Police and they do some work on them?

Simon Dukes (Chief Executive Officer, CIFAS): Yes.

Joanne McCartney AM: My second question, then, is wondering whether there is an issue with what a cybercrime actually is. You mentioned the definition. Is that creating issues and is this perhaps why the police do not necessarily think they have the skills? You talked about scams, but what is a 'scam'? It is quite clearly when you con people out of money or goods they do not get, for example, or you say it is a designer label when it is not. I know Caroline [Pidgeon] has done some work, for example, on a particular website that says, "We can get the congestion charge paid for you", and it will be £20. They do nothing different from what an

ordinary individual would do by clicking on the right website, but that is not criminal. Is there a definition problem we have with this as well?

Simon Dukes (Chief Executive Officer, CIFAS): I would be interested to know if there is. With this term 'cyber', how long do we have? It is sometimes a useful addition because it perhaps is more emotive and gets people's attention. However, what is it precisely? We are talking about fraud in this case, but we are talking about crimes that have been enabled by the internet. Actually, as we said right at the start, what that helps is for those crimes to be conducted at a greater pace and a greater scale, but the crime is still the crime. We must not get too focused on the fact that the vehicle being used is the internet. We do not talk about 'brick crimes' when someone smashes a window. It is merely the fact that we are looking at a vehicle in order to perpetrate something, whether it is a fraud or a scam of some kind.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Also, it is probably best to look at it as there is a black area, clearly, and a large grey one and some of the fraudsters actually prey on that as well. They deliberately create scams that are not entirely frauds but not entirely legitimate. That also helps them in terms of the potential consequences down the line because the victim will go to the police - and I have experienced this with lots of victims - and the police will say, "I do not think this is a crime. It is a civil matter". A lot of the fraudsters actually exploit that grey area. There are clear --

Joanne McCartney AM: Can you give us an example of what you are talking about and the grey area where the police will say it is not a crime?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): For instance, I interviewed a victim of a pyramid scam and she went first of all to the Citizens Advice Bureau and they said, "Well you have a fraud here", and therefore she went to the police and the police said, "No, this is not a fraud, this is a civil matter, you need to go to Consumer Direct". Then she went to Consumer Direct and then Consumer Direct said, "No, this is a fraud, you need to go to the police". She was sent on a merry-go-round. Now, I am sure there are lawyers that could probably fight either way, was it a crime or not, however as far as she was concerned she was scammed, she lost her money. Therefore I think there is this large grey area, which is exploited and we have to remember that, and we look at these types of things.

Caroline Pidgeon MBE AM: Also, I mentioned that we have this new Fraud and Linked Crime Online command, FALCON, how should the MPS measure the success of FALCON?

Simon Dukes (Chief Executive Officer, CIFAS): Well, presumably with fraud going down and victim awareness, or citizen awareness, going up. I am perhaps not best placed to try and say how either of those should be measured. I know I keep banging on about the citizen, however there really is - and I include SMEs in that as well - a sense of getting the citizen to have some ownership and awareness of the types of crime that are being perpetrated against them.

Caroline Pidgeon MBE AM: The greater awareness is the preventative role that we talked about earlier, as well as the particular target of fraud going down, and then to the satisfaction--

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): If money is no object then what I would say is you have a prevalence survey now and then you have a prevalence survey every so often to find out what the level of victimisation is amongst the population. I think that would be the kind of ideal scenario. However, it would obviously cost a lot of money. In the absence of that, I think, like Simon mentioned, those types of things. I would hope they do not get too

focused on the detection and conviction rates because those can be manipulated by the police, and also think about some of the other sort of disruption type tactics they can use and measurements like that. I think there is the ideal world and there is the real world, how much money is available.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): Yes. I think that there is a danger because of the way in which police tend to think of measurement and success, but the real work, which will be raising public awareness, a lot of which will depend on good partnership working. That has not come into the frame enough, but a lot of the people who will send out the messages most regularly that people will pick up will not be the police themselves. Therefore I think there needs to be very good partnership working, raising awareness and prevention, therefore you may have crime going -- you have your -- and I think in terms of ordinary everyday victimisation, we do have the Crime Survey and it has missed out very badly. However, of course, had it captured this in the same way as it captured card fraud that has kept it out of the reckoning, I am not quite sure that the Crime Survey would have been relied on so heavily by Ministers under two Governments now as proof that crime is endlessly falling. However, leave that aside, the Crime Survey should be picking up ordinary everyday fraud. That should be capturing ordinary everyday Londoners' experience.

However, certainly the sort of survey that I think you are talking about would be a good survey of businesses and particularly, maybe, the SMEs, starting with them. However, if you then find that the survey evidence shows that this is going down, the danger is that you will of course always have the police saying, "It was us that did it", whereas in fact hopefully it will be because citizens have received the message, they are taking their own precautions, and it is that raising awareness, which is what is doing the trick.

Caroline Pidgeon MBE AM: It is preventative for individuals, not businesses, that some of the Safer Neighbourhood Police, like they give advice on how to keep your home safe, that they could be giving out through Safer Neighbourhood Panels and other things, talking to people about how to make sure they are safe online.

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): I think a lot of the awareness among ordinary citizens now is coming to them in messages from Internet service providers and so on, there are a lot of messages coming through online, they are not coming through from the police. The police can add into that and every little helps, however I do not think they are going to be the main sources of raising awareness in people taking those sorts of precautions.

Caroline Pidgeon MBE AM: OK. My final question is, I think, Mark, you already touched on some survey work and more analysis of the problem in America and Australia, however what can we learn from international best practice on this, what are other forces doing, or even other forces in this country, although I am not sure there are any doing as much, however what can we learn?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think there have been some studies on Canada and there is I think Project Centre of Operations Linked to Telemarketing Fraud (COLT) and the Toronto Strategic Partnership, where they brought together all the key policing agencies, all the key government agencies, local government, as well as some of the private sector, and they worked very, very closely together in this partnership to tackle a particular problem at the time of telemarketing fraud, and it was a great success. They did all kinds of things, particularly disruption type techniques, therefore they hired students to phone up, who were the kind of target victims, and say, "Look, this scam is going on, we are the students, this is something you need to be aware of". It was a great success, therefore I think there are some great partnerships like that we can look to and I think that is a good example that it is worth looking into.

Caroline Pidgeon MBE AM: Canada seems to be leading the way. Simon, do you have any other good examples?

Simon Dukes (Chief Executive Officer, CIFAS): Nothing really to add other than I would say that, because of what we have seen, and because of the cross-sector nature of the type of crimes that we are looking at, then sharing good practice - I hesitate to use the word "best" because I think it is such a fast-moving environment here, I do not think we will ever get to best practice, but good practice - yes, absolutely, public sector can learn from the private sector and vice versa. Law enforcement, but also academia, and I am not saying that because my two colleagues are sitting here on my left, however we work very closely in CIFAS with academia because there is an awful lot that can be pulled from the data, from research, and from a particular academic approach, as I think has already come across here today.

Caroline Pidgeon MBE AM: OK. Marian, do you have any other international examples or others?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): No, not at all, however I do think the issue of partnership is finally coming out, and that has to be key. When there was a street crime crisis, a lot of what really made a difference there was target hardening, it was getting mobile phone companies in and finding ways of blocking stolen mobiles. It has to be like that and it cannot just be for the police, therefore they can take some initiatives and add to the pot, however it will not ever just be down to the police, and particularly maybe not in this area.

Roger Evans AM (Chairman): We have some questions about victims' experiences.

Tony Arbour AM: Are there groups or organisations, which are most likely to be vulnerable to this kind of offence? If there are, perhaps they are the ones who should be target-hardened in the way that Marian has been suggesting.

Simon Dukes (Chief Executive Officer, CIFAS): First of all, I think we are all at risk, and I think you are absolutely right to use the word "vulnerable" here. That I think goes back to the example that I mentioned earlier about the 55-year-old person who is perhaps quite savvy at share dealing, however gets scammed through a boiler-room scam, as the FCA have said recently, and there you have a particular vulnerability that these people who perhaps feel confident, perhaps over-confident, in that sort of environment. Therefore, there are different risks, risk exists, there are different vulnerabilities, depending on different scams, because fraudsters, criminals, are very clever at picking their victims.

Whether they be first-year university students; the classic case of the end of a first year and a student who has perhaps run out of money, it is getting close to Christmas, someone approaches them in the bar and says, "Give us your bank account details, we just want to put some money through it and we will leave £300 in your account so that you can buy presents for your family at Christmas". Of course the money goes through, the bank immediately spots it as misuse of facility, money laundering, the account is stopped, it is flagged as a money launderer's account. There is no money left of course by the criminal at the end of it and the poor student is flagged up as a potential money launderer as a result, and all the implications that will have for their credit history for the next two or three years. They are very clever at picking potential victims.

Tony Arbour AM: They are not the usual suspects perpetrating the crime, because is cleverness not exactly the opposite of "usual suspect"?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): There is a spectrum. The "usual suspect" is at one end of the spectrum, this is something that is happening further up

the spectrum. It is not either/or, I mean it does not preclude the fact that the usual suspects are also at it. They are not the ones that are doing this sort of thing.

Simon Dukes (Chief Executive Officer, CIFAS): Therefore, when you then have, as we are seeing, and there is some interesting research going on at the minute with the FCA and charities like Age UK, as to whether age has some sort of effect on vulnerability to online types of crime, and I think that research has not finished yet, however it will be interesting to see what comes out of it. However certainly there are certain groups of people who are targeted, again social engineering combined with online crime, because perhaps people who are retired may be more likely to be at home when the phone rings and the fraudster is at the other end trying to elicit personal details. Therefore all that sort of thing, yes, there are different types of groups more at risk and more vulnerable, and what we have to do is, like the criminals really, to make sure that they are aware of the types of crime that could be perpetrated against them.

In my organisation, we are particularly concerned with what we regard as people who are the most vulnerable members of society, people who are subject to court orders under the Mental Capacity Act, and we protectively register their identities on our database so that fraudsters are unable to put in an application, for example, for a credit card or for an online account through the system, so it hits the buffers and therefore those people's identities are protected. However that is just one small element of a massive project that we need to undergo in order to protect people. Sometimes they have to protect themselves, sometimes they can only do that with awareness-raising, and sometimes, in the case of this example, it is only going to be other organisations, perhaps businesses or Government, protecting people directly.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think it is better to look at it in terms of the fraudsters are very innovative and they develop frauds for almost every type of person there is. Therefore you have ticket scams, which are obviously generally focused at younger people, students. You have slimming scams focused invariably at women who are looking to try and lose weight. You have investment scams which tend to be more for older men. Romance scams, people looking for love. I have had a colleague fall victim to a *Who's Who* scam, because they played on the academic's vanity of wanting to go into *Who's Who*. There is a scam for every type of person and I think to say that there are certain groups, we are all vulnerable, we all have our weaknesses that we can potentially fall for in a moment of pressure, which we are often put under. I think that is the important thing to remember.

Tony Arbour AM: Can I ask a further question, and this I think has been hinted on when you talk about the embarrassment of your 55-year-old man who thought that he was savvy and thought he knew the score, "I am not going to be scammed by this goldmine in Valparaiso", kind of thing. Is that reaction to being a victim of crime different from the reaction that a victim of a more traditional crime has? In other words, are victims of more traditional crimes more likely to report them than people who are victims of cybercrime? It appears to be obvious but there may be lots of people who do not report being victims of traditional crime either, which I think goes back to your Crime Survey thing. Is there a difference?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): We do not know enough yet to be sure. In terms of impact on victims, it is always worth remembering though that we tend to think traditionally of the impact being much worse for victims for more serious crimes. Different individuals react very differently to different experiences. You can have a victim who is particularly vulnerable who reacts very, very strongly, so a relatively minor crime has long-term consequences for them. Whereas, someone who is a victim of what looks like a fairly serious crime may just say they have to just go on with their life. Therefore there is no sort of predicting how any sort of victim is going to react to any particular type of crime, and we simply do not know enough.

One thing that is worth bringing out, I think though, is your 55-year-old man, and so on. One of the reasons why - I think it is Yar who documents this - one of the inhibitors for reporting crime is that some of these scams, and I think that there has been a lot of comment about the fact that crime carries on going down against the odds because it was supposed to go up in a recession and it has not. The reason why property crime has always tended to go up in recession is that people cannot afford the same sort of things and the kids are still wanting the same things for Christmas and "how are we going to get them?" Therefore there has always been a large market for stolen, dodgy and illegal goods, and that expands when times are hard, it is not that people are reduced - by hunger and not being able to clothe their children - to going out to steal and rob. Therefore that is what you get now.

Where that has moved to - shopping around for bargains and so on - has of course been the Internet and that is not being picked up. Therefore I think that the recession effect is still there, it is going on to the Internet so that people are vulnerable where they are looking for bargains and so on. However, within that, you also get people who, when looking for bargains and opportunities for making money, and then get scammed, do not know whether they have been complicit in something that might have been illegal, and that is another reason why they are reluctant to report. Therefore you have that going on as well. I think that is worth putting on the table.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think another thing I would add is you have often very small sums of money and they think of all the hassle they have to go through to prove it and they think, "£20, £30, is it really worth it?" Therefore I think you have to throw that into the mix as well because a lot of these frauds are industrial scale, but lots of very small sums of money.

Tony Arbour AM: A thousand £20 scams.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Exactly.

Tony Arbour AM: Finally, in terms of victim support, do the victims of cybercrime need a different kind of victim support from victims of traditional crimes?

Simon Dukes (Chief Executive Officer, CIFAS): Again, I am perhaps not best qualified to answer this, however all I would say is, having spoken to some of the operators at Action Fraud and listened to a couple of the calls that they have taken, make no mistake, the victims of cybercrime scams are as distraught as victims of other types of crime, it seems to me. Given the high volumes of people being scammed in this way, it is very difficult to provide victim support on such large numbers; that is clear. However, I think there is some need for support or help or guidance, and whether that means, because of the nature of the crime, digital-type crime, whether there is a digital-type support mechanism, as referred to earlier, that we can somehow protect people's identities, with their consent clearly and their participation, by having them perhaps flagged in databases or with their bank that they might be potentially vulnerable to a particular type of scam or perhaps if they have a mental health issue, bipolar for example, that might cause them to spend in a particular type of extreme circumstances. These sorts of things we need to think more carefully about how we can protect people using technology more as well as providing support.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think I would agree in terms of just some of the victims I interviewed, some of them did not lose any money, however it was the mere thought that someone else had impersonated them, gave them a great deal of stress. Therefore I think it is important not just to focus upon the money, because I did interview some very distraught victims in that scenario. I think their needs vary, just like any other type of victim. The

survey that we did with them, one of the overall things was they wanted to find out what was happening, because invariably they report the fraud and then they never hear anything again, and just to find out if the police or whoever is investigating has actually done anything, if anyone has been identified, those basic types of information are very important to them.

Then of course there were some victims that clearly wanted more support. However, I think we also have to be careful in offering support to these victims, because if they have been defrauded by the Internet that often the solution is to provide support through the Internet, and some of them are obviously very put off by the Internet and some scammers impersonate some of these bodies to get victims. Therefore it is a difficult area to offer support. I know Action Fraud has done a lot to try and package that kind of support, however there is always more that we could do.

Roger Evans AM (Chairman): Have you found that victims worry that they are going to become victims again? Therefore you have been a victim of one act of fraud and you do not know what is happening to your details out there.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Yes, there were definitely some victims we interviewed whose behaviour had changed as a result; therefore whereas previously they might have bought holidays on line, now they are much more careful on how they purchase those types of things.

Roger Evans AM (Chairman): Yes, and if we had a victim who had been burgled, we would send the crime prevention people around to make sure their house was secured and also do some proactive work on the houses next door to ensure they were secured as well, because we know that burglars strike again in the same location. Is there any similar work done with fraud at the moment? Would it be useful?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think that would be very useful. I think you do for instance get some banks that do provide a very good service to their customers. That is one of the things we found out in our research that bodies are providing a lot of information, a lot of support, outside of the framework of the traditional agencies. However, I think particularly someone who has fallen victim, it has been quite a traumatic experience to them, and they are worried about further victimisation. Therefore, if you had the resources to send someone around to help them and to give them advice on how not to be a victim again, I think that would be great.

Roger Evans AM (Chairman): OK. I have some questions about reporting online crime. Obviously this is an area that we have covered several times during the discussion; so I thought I would just like to focus on the effectiveness of Action Fraud. I think the Deputy Mayor for Policing and Crime does not think much of it; he refers to it as "No Further Action Fraud" on the basis of a lack of follow-up of crimes. Mark, what is your feeling about this organisation? Do you think centralising the reporting of crime has improved the level of reporting and victim satisfaction?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Firstly you have to look at what it was like before Action Fraud and that was a mess in that you had those victim merry-go-rounds like I described. Those still happen, of course it has not got rid of that completely, however at least we do have now one body that, with the right resources and profile can, I think, get a much better grip on encouraging people to report and stopping those kinds of merry-go-rounds that we had in the past.

I think the problem is the expectations that Action Fraud has created because people think, "A nice central reporting body, I will report my fraud to them", and then they think it is going to be investigated and that

someone is going to get caught and there is going to be a case. Of course that is, in most cases, not what happens. The case goes into Action Fraud, it is packaged up into intelligence packages, which are then sent out to the police forces, and they prioritise those and therefore a lot of frauds just get lost in that bureaucracy and the victims obviously get very frustrated, understandably so, "I have reported this fraud, I expect something to happen, and nothing is happening".

That for me is the main issue that I pick up with Action Fraud. That is not to say there are other things that need to be assessed on its effectiveness. When Action Fraud was set up, and I originally did the research for the National Fraud Authority, originally there was going to be the first part of the research and then there was going to be a second follow-on part of the research to evaluate Action Fraud. However, with all the kind of cuts in Government, the second part of that evaluation was cancelled. Therefore, as far as I am aware, Action Fraud has never been evaluated by researchers.

Roger Evans AM (Chairman): There was a caveat in what you said to me earlier where you mentioned that in fact it could be successful with the right level of resources. Are they overloaded with work?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I visited Action Fraud in the City of London Police and it was a huge room, probably as big as this, and I assumed it was all Action Fraud. I thought, "This looks really good, all these people", however most of the people in the room were the National Fraud Intelligence Bureau, and it was a tiny proportion down one end.

Roger Evans AM (Chairman): They are the people they report to?

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Yes.

Roger Evans AM (Chairman): At least they are in the same room.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): Yes, but when you talk to police officers, I still pick up anecdotal evidence that they do not know what Action Fraud is and, therefore, I think there still is a message to get out to police officers and to the other agencies that there is this body and it has taken on the main role. It is like any kind of change like this, it takes a long time for everybody to realise that this has happened.

Roger Evans AM (Chairman): I think the Working Group may decide to have a visit to Action Fraud.

Tony Arbour AM: It is obviously not going to take very long!

Roger Evans AM (Chairman): The sort of visits we like! Just finally --

Simon Dukes (Chief Executive Officer, CIFAS): I just wanted to be the defender of Action Fraud really because I do think that it --

Roger Evans AM (Chairman): You think the Deputy Mayor for Policing and Crime's characterisation is unreasonable?

Simon Dukes (Chief Executive Officer, CIFAS): I do. I think Action Fraud does a very good job. It makes it very straightforward for a citizen to report a fraud or a scam. They get a crime number; they get advice; and that information, as Mark [Button] said, goes straight through to City of London Police and it is packaged up.

It is then sent out to the relevant forces. That is where the action aspect should be taking place. That is where the resource issue is, not, I would suggest, with the reporting process and the fact that the frauds are going through, but the fact that you are dealing with hundreds of thousands of crimes every year, no police service, however well resourced, in the UK is going to be able to deal with that, I would suggest. Therefore, even one organisation like CIFAS, I have talked about 1,000 crimes a day that we have, that is more than West Midlands Police deal with in a year. We deal with more. Therefore that is the level that we are talking about; therefore I think Action Fraud itself does a good job at funnelling in. Yes, of course it could do more to publicise it, but it is then what happens next, what happens once the fraud has been reported.

Roger Evans AM (Chairman): Yes, it is probably a question for the MPS rather than yourself, however do you know if the Commissioner's commitment to have every victim of crime visited by a police officer in London extends to what is passed on by Action Fraud?

Simon Dukes (Chief Executive Officer, CIFAS): Indeed.

Joanne McCartney AM: We can see from their website, they say they partner with Victim Support.

Caroline Pidgeon MBE AM: I had never heard of them I am afraid.

Roger Evans AM (Chairman): I had never heard of them either, however we spend all our time in the basement.

Just finally, thank you for your evidence today. Do you have any suggestions what further steps the Mayor and the MPS could take to improve the reporting of online crime?

Professor Marian Fitzgerald (Visiting Professor of Criminology, University of Kent): If anything comes to me I will write to you, I promise.

Professor Mark Button (Director of the Centre for Counter Fraud Studies, University of Portsmouth): I think just clearly more campaigning to encourage people to report, because obviously the better handle we get on the scale of the problem, the better we can deal with it. Just quickly, just like Marian, I will write to you as well. However I think more campaigning to encourage people to come forward, even those small frauds, because at least then, if you have that kind of evidence coming, you can do an immediate campaign, "There is this type of fraud happening"

Simon Dukes (Chief Executive Officer, CIFAS): Only what I've said already the work that Mandy Haver-Little is doing. The working title is the London Digital Security Centre. It may change. This MOPAC initiative in order to help improve cyber security awareness, working closely with Metropolitan Police and MOPAC I think is an excellent initiative. I think if we do that right it well help to improve knowledge and awareness of the problem and therefore improve reporting as well.

Roger Evans AM (Chairman): We end on a positive note. Can I thank you for your very useful evidence? The purpose of this session is to scope out the problem and also to think about the questions we will ask the enforcers when they appear in front of us at our next meeting. You have given us plenty that we can raise with them.