Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 24 March 2022

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Lord Allan of Hallam; Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; Lord Gilbert of Panteg; Baroness Henig; Baroness Kingsmill; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 7 Virtual Proceeding Questions 61 - 69

Examination of witnesses

Kathryn Westmore, Dr Alice Hutchings and Dr Konstantinos Mersinas.

The Chair: Good morning and welcome to this evidence session of the Select Committee on the Fraud Act 2006 and digital fraud. A transcript of our meeting will be taken and published on the committee's website, and you will have the opportunity to make corrections to that transcript where necessary.

Thank you to our three witnesses for this morning's first session on cybersecurity. We are delighted to be joined by Kathryn Westmore from RUSI; Dr Alice Hutchings, director of the Cambridge Cybercrime Centre at the University of Cambridge; and Dr Konstantinos Mersinas, senior lecturer at Royal Holloway. Lord Vaux will ask the first question.

Q61 **Lord Vaux of Harrowden:** I start by asking you to give us a description of what the cyber-fraud landscape currently looks like and how it has evolved over time. Looking forward, what sorts of threats do we face from emerging technologies such as the dark web, malware, ransomware, crypto fraud and presumably others? If we can start with Dr Mersinas, that will be terrific.

Dr Konstantinos Mersinas: That is a great question. There are two angles to consider here. First, we see that tools are being made increasingly available, so we have the notion of crime as a service or

ransomware as a service, which means that non-technical individuals can go online, possibly to the dark web, and obtain these tools. That means that the previous requirement of having expertise and special skills for hacking or fraud is not necessarily needed any more.

At the same time, we also see a pattern of increasing organisation. We recently saw that a few days ago with a group called Konti in Ukraine. With these structures and hierarchies, which are businesslike and very well organised, criminals are creating new branches here and there. We see that they have special departments to deal with open-source intelligence, releasing videos, getting feedback from security professionals or researchers online and so on. It is these two aspects that we need to consider in the current landscape.

Lord Vaux of Harrowden: I am interested in your comments about Ukraine. Is this primarily an international problem? How much is UK-homegrown and how much is international?

Dr Konstantinos Mersinas: That is a good point. I think it makes most sense to talk about it on an international level, not a country level, but of course these groups will have specific interests here and there. In general, if we are talking about the motivation behind this organised crime, which is mostly but not necessarily just financial, we should be considering it at a broader level. I think it is closer to an international level than a local one.

Lord Vaux of Harrowden: Dr Hutchings or Kathryn, do you want to add anything particularly about the landscape and evolving threats?

Dr Alice Hutchings: I will be a bit controversial here and say that it has not changed that much. The landscape has certainly changed in some ways—we have more mobile devices and increased popularity of cloud services. However, a review by Anderson et al looked at how the cost of cybercrime had changed from its first paper in 2012 and found that the landscape looked remarkably similar; the vast majority of online cyber frauds still accounts for very small value but very high volume. This has remained constant compared with offline traditional frauds, which tend to remain very high value but low volume.

We see the reverse in defence costs. For online crime, the defence cost is much higher, even though the criminal revenue might be relatively low. It is possibly in things like ransomware where we see differences in this general pattern. Ransomware is certainly a really big problem. One of the problems with it, again, is the defence cost. It is not necessarily how much ransom is being demanded—hopefully, people are not paying those ransoms—but the cost of recovering: restoring from back-ups, cleaning servers and so on. That seems to be the biggest impact on organisations.

You mentioned crypto fraud. We see this as another emerging area, and we are doing research on it at the moment. Cryptocurrencies are linked to other types of fraud: fraudulent exchanges and exit scams have been a big problem, fraudulent initial coin offerings have been a big problem,

and there are also high-yield investment programmes and Ponzi schemes.

I will also be a bit controversial and say that the dark web represents a bit of a moral panic. It is seen as a big scary place, but the Tor network, which is what most people think of as the dark web, has many legitimate and useful purposes such as obtaining information in oppressive regimes and its use by journalists, whistleblowers and the like. There are many useful purposes for such a network.

When we talk about cybercrime in the dark web, we see mainly drug crypto markets. It is hypothesised that these can lead to the lowering of street violence that can be associated with street-level drug markets.

The other interesting issue is that a lot of cybercrime markets do not necessarily operate in it. Some of the crypto markets have cybercrime products and services available on them, but a lot of the more specialised cybercrime markets operate on the open web, because the administrators can control access to the marketplaces based on IP addresses using a block list to stop researchers like me from being able to go in easily and scrape and gain access to the data held there, which makes it a bit more difficult for us when things are hosted on the open net.

The other interesting thing about the dark web and fraud is that this is not a place where traditionally scams take place. There are scams there, but they tend to try to scam people who are using the crypto market—for example, by phishing to pretend that you are a drug market to get people's credentials. So it is a bit different.

Most fraud takes place on the open web. Often, use is made of compromised web pages or social media platforms. The dark web is a bit of a bogeyman of crime. Is there anything else you would like to follow up?

Lord Vaux of Harrowden: No. That is very interesting. Kathryn, do you want to add any brief comments?

Kathryn Westmore: I think both answers so far are absolutely right. From my perspective, what has happened particularly with cyber fraud and online fraud is that fraudsters have just followed us online. They are very much driven by the behaviours that we exhibit, because that is where they sense the vulnerability and the gaps. When we talk about things like crypto fraud or fraud in the metaverse, as a fraud practitioner the frauds in those areas are still the traditional types of fraud; they just have a cool new word attached to them, which often lures people in for investment scams, for example. I am sure most people have seen horrendous stories in the news about people losing large amounts of money to crypto investment scams. Although that has the buzzword "crypto" attached to it, it is very much a traditional investment scam of the type that has been around for years and years.

When we look at the cyber fraud and online fraud landscape, we have to look at the landscape of our own behaviours. When we are trying to look forward to what the fraud landscape will look like in 10 or 20 years, a lot of that is trying to work out what our own behaviours will look like, particularly in how we share personal data, which is crucial to the operation of a lot of these online fraudsters.

On the other point that was raised is the excellent question about whether the threat is international or comes from within the UK, this is an area where the threat needs to be better understood, particularly the location of perpetrators. It is an area where our intelligence community and the resources that we have could be used and positioned well to face the threat.

Q62 **Baroness Henig:** Perhaps we could ask more about the perpetrators themselves. I think Konstantinos suggested that they were more international than UK-based, and we would like to hear a bit more about that. Are we talking about lone individuals or crime gangs? Is there a normal pattern here or is it completely random as to who is doing the crime?

Dr Alice Hutchings: In relation to organised crime, it depends how you define it. If you look at the UN definition, you can probably argue that many crimes are organised, but if you talk to a criminologist they will say something a bit different. Organised crime tends to have a level of governance and control. Traditional organised crime groups operate through the threat of violence: "If you do me wrong, you'll have a broken leg". It is a lot harder to do that when you do not know who your co-offenders are, where they are located or where there is a physical distance between you.

There are different ways to try to slice the apple here. You tend not to see online-only groups being too involved in organised crime in that regard. What you see perhaps are some traditional organised crime groups starting to move online and look at the money-making potential there, but a lot of these operate in local communities as well. There tend to be local business approaches. What we see very much online is co-offending. That is not necessarily organised crime through the level of governance, but it means that people can be specialists and we see supply chains.

Going back to the well-made point earlier about crime as a service, we can see people creating crimeware. People use that to compromise credentials. Those credentials may then be traded, and other actors use the credentials to monetise them and cash out. There is a whole level of different services being provided at different points in the supply chain. You do not necessarily see the same actors involved in the whole process. In some ways they can distance themselves from the use of those compromised credentials.

The question as to where offenders are based is a really difficult one if they have good operational security skills. Often, the location where it

appears the attack is coming from is the location of a compromised device or server that is being used as a proxy by the attacker. It can be quite difficult if you do not have the resources to do proper in-depth investigations to find out where attackers are based. This is not generally done at scale but for particular investigations where you might be able to locate where an attacker is based on evidence from different countries. It can be quite difficult to find where offenders are.

In many cases of low-value fraud, the attacker probably is in the UK. They may be using services based offline, but for things like accommodation frauds and frauds related to trading sites and so on, many will be based in the UK, but they are never investigated because the value of the fraud is so low that the police do not have the resources to investigate them and they basically operate with impunity—and that is here in the UK.

Kathryn Westmore: I absolutely agree with that, particularly on the lack of intelligence. We can certainly see a large degree of co-operation and co-ordination between some criminals. That is evidenced, for example, in the rapid mobilisation of criminals in response to things like the Covid-lending schemes. They were able very quickly to exploit the gaps in the schemes and obtain fraudulent funds. Something like that really shows that there are groups of people working together to share credentials, information and data. I think that is driving a lot of this. I reference the high-volume, low-value fraud that we all experience constantly. It is always in the background. That certainly has the hallmarks of organisation, if not technically organised crime.

Baroness Henig: Often it is well-established groups that move into new fields.

Kathryn Westmore: Absolutely. There are some examples particularly in west Africa. Some of the organised criminal groups there operate across a range of different types of criminal behaviour. They use fraud almost as a way of subsidising their running costs, because it is low risk for them. Somebody can spend an afternoon in an internet cafe sending out romance fraud emails, for example, and that subsidises some of their other activities, because it is a good return for relatively low risk; they do not really fear the consequences.

Dr Konstantinos Mersinas: On the question of the landscape, I think it makes sense to view cybercriminals, whether they operate on their own or in an organised group, in a sense as entrepreneurs and start-ups, because this is what they do. We had, for example, the case of Daniel Kaye, a British citizen, who was arrested in the UK. He launched all the attacks from his mobile phone in Cyprus at the time.

We have mentioned the different levels of skills and engagement of the supply chain; you have the developers, the people with the knowledge and expertise, and then you have the potential clients and start-ups. All of them, either on an individual level or on a group level, have to build a name and promote their products, and they have to make sure that their

products are reliable. Clearly, we are talking here about business terms. All these individuals are bound by the same market restraints that normal software groups would be bound by or that they need to achieve. They need to build a name, establish themselves and find ways to take their business further.

We know that in ransomware cases there are client support centres in India, for example. These guys did not know that they worked for a ransomware organisation, but they assisted people on how to buy bitcoin and things like that. Therefore, in my view, it makes sense to view them as entrepreneurs and start-ups.

The Chair: That is very helpful, and very concerning.

Q63 **Viscount Colville of Culross:** Dr Mersinas, I would like you to explain how technology can be used in counter-fraud policy. Traditionally, machine learning has been used by financial institutions, but I understand that is not enough. Could you explain to us what deep learning is and how this can be used by financial institutions to try to deal with the problem of fraud?

Dr Konstantinos Mersinas: A couple of words here. First, machine learning can, of course, be used for the legitimate purposes of marketing and entertainment, in coping with fraud, and with the opposite goals in mind. We are at the stage where the technology still has many false positives and many false negatives. Incidents are incorrectly marked as real incidents and vice versa. We are still bound by historical data. We are still bound by simulations and exercises. In that sense, we are not there yet.

One general trend I would like to mention here is the notion of explainability. This would allow for some transparency and understanding of the algorithms. That is the next general trend that we need to focus on. The practical application of this is a more complicated question.

Viscount Colville of Culross: Could you also talk to us about deepfakes and synthetic identity fraud? I understand that Microsoft and Facebook support something called the deepfake detection challenge, harnessing this technology to be able to deal with this sort of counter-fraud. I would be very grateful if you could talk to us about that.

Dr Konstantinos Mersinas: I think the focus should be broader than face-swapping applications. The ideas under discussion at the moment are mostly dominated by face swapping. We should have a broader view on that.

Let me make a parallel here. Recently, with regard to the online harms Bill, we had consultations about IoT and the risks to consumers. It totally makes sense if we have providers, organisations and agencies taking more responsibility—you mentioned Facebook and so on—for the protection of people and individuals who use their services. Of course, that is a big discussion, but we are already moving in that direction. I do

not know if the word "strategy" is right, but there has been a strategic view in the UK already, and that is a very good sign.

Viscount Colville of Culross: Alice, do you have anything to add about the importance of moving on from machine learning to try to deal with some of these frauds in financial institutions?

Dr Alice Hutchings: Machine learning is used successfully every day in detecting and preventing fraud. The vast majority of email that is sent around the world is spam and fraudulent, but these do not appear in your inbox because of machine-learning algorithms. You just never see them. They do not even go into your spam folder. Most of them are detected as being spammy and blocked totally.

As has been mentioned, false negatives make their way into your inbox and into your spam folder. Often you will detect these and people use the "report spam" button. That is then used to train the machine-learning algorithms to detect other emails that people do not want to receive. You are actually training an algorithm when you report spam. What can be more painful is the false positives, as mentioned, where the mail you want gets relegated to your spam folder. I am sure that has happened to many people.

Machine learning generally uses two approaches for detecting fraud. The first is understanding the behaviour of legitimate users—legitimate account holders, users on a platform: for example, credit card holders—and detecting patterns that are inconsistent with their use, with their normal behaviour.

The second is detecting patterns that are indicators of criminal activity such as compromise. In addition to things like spam detection, these include detecting compromised credit cards, compromised online accounts and online access to computer systems. Antivirus software, for example, uses machine learning to classify the activities of malicious applications. We then see—this is a bit of an arms race—attackers or offenders displacing their activities to circumvent these machine-learning algorithms. In some cases this can include things such as loopholes. If there is online detection on a merchant, they might ring up and do the fraud by phone, because potentially telephone transactions are not being checked.

I do not think we are seeing deepfakes so much as people trying to imitate genuine customers in some ways, such as by having an IP address that is in the same region as the customer. We are seeing less technical means that are just as effective at overcoming those types of algorithms.

The more complicated technical approaches are not likely to be used in favour of relatively straightforward, non-technical attacks. Things like using insiders in organisations is much less complicated but much more effective than using a deepfake approach. I see some movement towards deepfakes, but this is a particular type of fraud simulating sex workers

online. This tends not to get reported to police by the customers, who perhaps would be seen as being in compromised positions.

Viscount Colville of Culross: Thank you very much. Kathryn, briefly, can you talk us through the next generation beyond machine learning—the importance of using deep learning and just allowing the machines to take over to an extent in dealing with frauds, particularly in financial institutions?

Kathryn Westmore: There are some incredible technologies being developed, particularly in the private sector, using things like deep-learning tools. The benefit that comes from that is removing some of the routine processes and allowing humans to focus on the higher-risk areas. It is about automating those tasks. We have already talked about false negatives and false positives. By reducing the number of false positive results, it allows the human investigator to focus on the higher-risk areas and to waste less time, frankly.

In all these technologies and the advances in fraud prevention and detection technology, for me the real benefit will come when there is more cross-industry and cross-private and public sector data sharing. At the moment, that limits the effectiveness of some of those technologies to a certain extent. As we move towards a world where more of that data sharing is happening—it is early days, but it is beginning to happen—that is when we will see some of those technologies really come into their own. Any single institution only has part of the data view. Being able to combine its data with data from the public sector, other institutions and technology companies will allow some of those technologies to add value and benefit in fraud prevention and detection.

Q64 **Lord Sandhurst:** Dr Mersinas, you in particular have observed that blacklists operated by platform providers such as Google Safe Browsing can help protect against phishing attacks in two ways in particular: by warning an individual user that they are just about to enter a dangerous site or download a dangerous file, and by notifying the relevant webmaster when a website has been compromised. How effective are such efforts to protect consumers? How can we measure the success of counter-cyber-fraud policies? Are there any really good means of doing this?

Dr Konstantinos Mersinas: That is another difficult question, of course. Every measure and every approach is welcome, and it all helps. That is a useful approach and it should continue. However, there are always limitations to all these approaches, and the reason is this. The problem here is not a technological one but a matter of human behaviour. We observe that knowledgeable people and even security professionals might fall for attacks like that, users ignore the notifications that they receive in that fashion, or they do not know what they mean. Even if they have a sense of what they mean, they might still continue with some action for a number of reasons.

Measuring their effectiveness is one thing, because we need to know the space of the events, we need to see how many events actually take place, and so on. That is not easy, because we have a problem of reporting—basically, underreporting—unless it is somehow measured technologically. It is a matter of behaviour and somehow changing the behaviour of users. The fact that security professionals might fall for social engineering attacks in particular, and phishing, indicates that it is not a matter of knowledge or of providing the information. We have an understanding, at an academic level, of the psychological principles underlying human behaviour, but this needs to be embedded more in the approaches. We need to understand that time limitations, cognitive limitations and lack of information all combined might—and do—lead users to fall for phishing attacks and social engineering. My point is that there are real limitations there.

Lord Sandhurst: So it is education and culture, looking forward. Is that because it is all relatively new to us; it has only happened in the last 10 years?

Dr Konstantinos Mersinas: It is education. Usually this is phrased as security awareness training, which in my humble opinion is not the most accurate term. We should look not just at awareness or at education, but for ways to change the behaviour of individuals, users and people in general—a way of habitualising more secure behaviours among people. That is a very important angle, and there should be a focus on the individual.

Lord Sandhurst: Your university has done some research in the past looking at Twitter's URL-shortening service, which is designed to protect users from phishing and malware attacks. How effective is that at the moment?

Dr Konstantinos Mersinas: I cannot comment on the effectiveness of that specific approach. Again, not all approaches are of the same level. Increasingly, we see approaches that include these factors, but, if you have seen the surveys, by and large the industry still relies on what I call traditional security awareness training, which is probably not the best term, as I said, which has to do with annual training by video and information provision. They include scenarios that make things more vivid, and they personalise things so that it is easier for people to remember and understand and relate it to their personal situation, or the personal value of information, and so on.

Lord Sandhurst: Putting it shortly, is there one thing that you would ask us to recommend the providers change in their approach, which, if they did it, would mean that we were all much better off?

Dr Konstantinos Mersinas: If I were to put it in one sentence, I would say focus on individual behaviour, so that we have behaviour change with regard to security.

Dr Alice Hutchings: I take a different stance on this. I believe that the most effective anti-fraud interventions will be the ones where the users never even see the fraud. The email does not reach them, the advertisement has not successfully been placed, and they do not actually have to make a decision because the fraud has been stopped at an earlier stage.

In relation to how to measure this, there are things such as website takedown. It is a measure that is used in the phishing space for how long websites are active before they are detected and taken down, so that when somebody goes to enter their credentials on the web page it is no longer there. We see quite a successful ecosystem in relation to things like phishing, because there is a high level of incentive for banks to take action here. There is a whole industry of specialised companies that work with banks, hosting providers and registrars to take down phishing pages quickly. The measure of success is how long they are active for and how much visibility that crime has.

Lord Sandhurst: What single thing or two things should be done that would be effective? In other words, should the regulators or the lawmakers say to the proprietors, "You've got to do this"?

Dr Alice Hutchings: There needs to be a change in incentive. Problems usually occur where people are not incentivised to take action. One example is Google, in the US a number of years ago, being fined $500 million for allowing pharmaceutical companies to place advertisements using Google search terms. Google now has an incentive to ensure that unlicensed pharmacies do not use its advertising platforms. One way Google does this is to have a list of regulated pharmacies that can operate in the US.

Another area I have done a lot of research in is travel fraud—compromised credit cards being used for travel and in other types of crime. Again, this is a very highly regulated area, in that if you operate a travel agency or an airline, there is a lot of regulation and there are lists of regulated companies. Fraudulent travel agencies can still place advertisements on places such as Google, because Google does not necessarily have an incentive to ensure that those who place advertisements for travel services are legitimate.

Lord Sandhurst: Strict liability is the answer, is it not?

Dr Alice Hutchings: I am not quite sure about strict liability.

Lord Sandhurst: Strict liability for Google, for example. If it is provided and it happens, you have to pay the fine.

Dr Alice Hutchings: We are not necessarily looking at a one-off. We are looking at how to make companies such as Google change the way people can buy advertisements on their platforms and check whether they are fraudulent. In many cases, there are not going to be regulated lists of organisations such as with pharmacies or travel agencies, and it

can be really difficult for platforms to know whether a particular store is legitimate or not. I recognise that there is a big problem in establishing trust. You can look at trust signals and reputation signals, but this makes it very hard for innovation and new companies to come in and start being able to advertise to customers. It is not a straightforward problem to address, but it is certainly one that could have more attention paid to it.

Q65 **Baroness Kingsmill:** I wanted to talk to you, Kathryn, about the Government's response, how effective it is and whether you have any other suggestions. Are the national cyber security strategy and the National Cyber Security Centre good enough? They have good intentions, but are they focusing sufficiently on the right issues, and are they effective?

Kathryn Westmore: That is an excellent question. For me, taking it a step back, you have to look at the distinction between cyber dependent-type attacks, things such as ransomware and malware, which are very much reliant on that technology, and the cyber-enabled frauds. I am thinking about things like romance frauds, which are operated online, or online adverts for investment scams.

On the cyber dependent-type attacks, I think the strategy and the work of the National Cyber Security Centre is pretty good. Some of the weaknesses are on cyber-enabled frauds, which are the ones that as consumers we tend to notice more because we are being attacked through scam text messages, adverts or emails, for example. I think there is a lack of centralised response to dealing with those kinds of frauds that falls somewhere between the cyber world and the broader fraud world. Elements of it are picked up in the work that the Home Office is doing on fraud, for example, but it is quite a fragmented response, which obviously limits the effectiveness and the ability to take a whole-of-system approach to those types of cyberattacks. That then trickles down into the way the companies deal with those two different types of cyberattacks.

I think the National Cyber Security Centre has done a good job on some of the awareness-raising campaigns. Its Cyber Aware campaign is very sensible, and I imagine we will talk about the effectiveness of those kinds of campaigns later. Certainly more can be done to address those cyber-enabled frauds from a centralised perspective. That would certainly be my take on it. There is a need, given how prevalent those types of cyber-enabled frauds are, for a really coherent cross-government strategy that looks at frauds against individuals, businesses and the public sector, many of which are now cyber-enabled.

Baroness Kingsmill: Do you think they need to be more systematic about the kinds of areas that they are tackling—not so much the different kinds of fraud themselves, but the way in, if you like, to the different sections that you describe?

Kathryn Westmore: Yes, absolutely. As everywhere, there are limited resources, so I can understand why there is a focus on the

ransomware/malware-type attacks, which can be incredibly disruptive, as we have seen, but it is a slightly different skill set when you are looking at the cyber enabled-type fraud. Whether the responsibility for the government response to those frauds should sit with the National Cyber Security Centre—and I know other committees have talked about creating economic crime departments or bodies to look at the problem—or whether it sits somewhere else, there certainly needs to be a more coherent, government-level strategy to tackle those online-enabled frauds.

Baroness Kingsmill: We have had discussions as to whether we should look at the sorts of fraud that affect huge numbers of people but perhaps are relatively small in monetary value, or whether we should look at the big, massive frauds against the public sector or banks, or whatever. It is quite an interesting issue for us to consider. Do you have any comments on that at all?

Kathryn Westmore: I think that is a question for this committee to discuss, but it is a broader question, to be honest, when we look at the UK's fraud prevention and detection strategy as a whole. There is a lack of broad understanding of where the biggest threats are, and what has the biggest impact, and therefore where the limited resources are best targeted. As you say, is it on all the organised high-volume scams, or is it on the single big scam, or should we look more in particular areas? It is not necessarily clear to anyone where the biggest risk is, where the biggest threat is, and where the biggest impact to the UK is, and therefore what the focus of our efforts should be.

It is an excellent question and one that counter-fraud professionals have grappled with for many years when it comes to the definition, what is in scope and what is out of scope, when they are trying to deal with it and the different ways in which these crimes manifest themselves.

Dr Alice Hutchings: We have not mentioned Action Fraud, which I think is the elephant in the room. I was really pleased to see the commitment to replace Action Fraud in the beating crime plan last year, but this does not seem to have been reflected in the national cyber strategy, which I find a bit puzzling. I think it has perhaps been watered down a bit. I think low-value, high-volume crimes are destined to slip through the radar, and I would welcome any attention that can be placed on this problem. These can have huge defence costs, as I mentioned. Even though the value is very low, the cost overall is massive. This is a really big problem that is overdue some attention.

I wonder whether the police are empowered enough. I worry about the current arrangements, with ROCUs sitting in between local police forces and the National Crime Agency, and how this could hinder local police pursuing investigations locally. It has to come to the top of its priority list, come to the top of the ROCUs' priority list, and then to the top of the NCA's priority list. When you look at these low-value frauds, this is perhaps where we start to see investigations breaking down at a very early stage. It seems to be a considerable hindrance, and anything that

can make this smoother would be welcomed.

The Chair: I will bring in Lord Browne, because I suspect we will carry on in this vein and talk about culture and action.

Q66 **Lord Browne of Ladyton:** We certainly are in this vein. In fact, we have been in this vein since the beginning of the evidence session, but perhaps for a couple of minutes we could focus our minds on just how effective counter-fraud strategy is in prevention and detection. Why is it so ineffective? I think we should just be honest about it. It is pretty ineffective, certainly in terms of the scale, and the scale of the consequences of this for the United Kingdom.

Is it fundamentally about governance, co-operation, resourcing, lack of regulation or legislation, or is it all of the above, which I suspect it probably is? When you identify the problems, you might slip in some suggestions of solutions.

Dr Alice Hutchings: I think you have given a pretty comprehensive overview there. Resourcing is a big issue. The thing I would like to slip in is changing incentives to ensure that platforms are incentivised to try to disrupt crime at a very early stage in using the systems.

Also, people find it really hard to report crime if it is through Action Fraud, going to the police or trying to report it to the banks. When incidents are reported, usually nothing happens and it is not investigated. Again, this is a resource issue, but it adds up when you are looking at this by volume, and these types of crimes are volume crimes.

Lord Browne of Ladyton: Kathryn, RUSI responded to this national strategy by referring to it as an alphabet soup, among other things. There seems to be no shortage of initiatives that have developed into elements of what we do, but I have no idea how they fit together, and I have spent the last few months reading lots of briefings on this. I do not even understand what they all do. How do we make them more effective? Are we really going to make progress trying to make things that exist and do not work change to fit the challenges we see, or would we be better starting from scratch?

Kathryn Westmore: Exactly as we said, it is an alphabet soup, and, like you, Lord Browne, I have struggled to work out exactly which group of people is responsible for what. Where some of the groups have really had merit is bringing together particularly the private sector and the public sector in those forums. I am always slightly sceptical, though, about just creating more forums where people will sit around and discuss the issues. There will be vehement agreement that something needs to be done and another meeting will happen three months later, and that is the sum total of the output. I do not think that adding more bodies or groups to this will necessarily make any difference.

The Joint Fraud Taskforce and the Online Fraud Steering Group are all doing some really good work. From my perspective, bringing all those initiatives together, potentially reducing them, but actually making it

clear who is responsible for what types of fraud, with coherent leadership and governance at a senior level in government, would be a much better approach than creating more talking shops where everybody can sit around saying how terrible fraud is.

I am of the view that we probably need to look at the initiatives in the cyber world and at some of the initiatives that the Home Office is leading on, and the Cabinet Office are leading against public sector fraud. In the Spring Statement there is more money for countering public sector fraud. How does that fit in with other work that is going on in the counter-fraud space? It is certainly not clear to me. Given that there will always be limited resources, having a more streamlined approach will be far more efficient and effective at actually making changes and moving the dial, as you started off saying. It is evident from the statistics that interventions so far have not made a huge difference to the volume and value of the frauds that we see in the UK.

Lord Browne of Ladyton: Konstantinos, you suggested earlier that we should habitualise or normalise more secure behaviour. There are lots of areas where we are now challenged by normalising behaviour. On climate change, for example, apparently some 60% of it is dependent on people changing their behaviour. Whose responsibility is that, and how do you do that? You push this fairly strongly, so you must have some ideas.

Dr Konstantinos Mersinas: I think you are right; it is not easy. The art and science of creating a habit is not easy, but we have some insights from research that are quite counterintuitive. For example, behaviour needs to come first and then certain perceptions change. That is totally the other way round from what we tend to think. It is a massive problem that you are asking about. On what level should it work? We need to start with education early on. We have been involved in cybersecurity programmes with young people and school students, but equally, as mentioned earlier, there needs to be responsibility in the platforms.

As with other types of crime such as content crime, cyberbullying and cyberstalking, fraud has a similar angle in the sense that—let us be honest—law enforcement and Governments on their own cannot cope with what is happening here. We really need to have the technological giants, the ISPs and the platforms on board. A collective effort is needed here. I do not think anyone is under the illusion that it will work just by law enforcement efforts.

There is an angle here that I understand that has to do with the ethical considerations of behaviour change, but this is not a big obstacle. We can work it out. There are ethical ways to nudge and direct people to take voluntary actions towards more hygienic security behaviour. It works on many levels. I know that this is not a very specific answer, but I think it is the only honest one if we are to change behaviours.

Lord Browne of Ladyton: Thank you for your honesty. If you could point us in the direction of any society in the world that is doing this well, it would be really helpful.

Dr Konstantinos Mersinas: Human behaviour is mostly universal, by and large, so I do not think there is an example there, but some interventions work better than others. We can provide this evidence in writing if it helps.

Lord Browne of Ladyton: Thank you very much. Dr Hutchings, you may be able to help us out in a couple of sentences.

Dr Alice Hutchings: There are some issues here. Fraud changes very frequently, and often the message given in fraud awareness campaigns is not consistent with how people live their lives. Telling people not to click on links or not to open attachments does not work when people's jobs require them to click on links and open attachments. Sometimes this leads to victim blaming—"You should've been aware that this was dangerous"—but the advice has not kept up with people's realities. Bombarding people with messages leads to fatigue and to people ignoring things after a while. Companies intentionally phishing their employees leads to resentment and mistrust. There is a space for awareness campaigns, but it is certainly not going to be the answer to this problem.

The Chair: That leads very nicely into Baroness Taylor's question.

Q67 **Baroness Taylor of Bolton:** Some of my question has been answered, because I was going to ask you how successful you thought public cyber awareness campaigns were. This is a very important area, because you have already said that a lot of very small-value crimes occur at the high-volume end, and that really has a big impact on the individuals involved. It is not just a sum of money that they have lost; it is very often their pride, and they feel gullible and stupid. People need some protection.

If the campaigns that we have seen have not been very successful in changing behaviour, as Dr Mersinas says is necessary, what do we have to do to give people more protection? Who might people listen to? Do they listen to the public awareness campaigns, or do they listen more to some of the television consumer programmes or some of the experts such as Martin Lewis? If we will get the right interventions, where are they going to come from?

Kathryn Westmore: You make excellent points about the effectiveness of awareness campaigns. I will fully admit that I have worked in this space for 15 years, and I know what I should do, but I have probably hundreds of compromised passwords; I have alerts that flash up on my phone telling me this, and I just ignore them and think I will deal with it another day. I am aware of the awareness campaigns because I work in this field. There are lots of people who are not even aware of awareness campaigns. Awareness campaigns have not changed my behaviour particularly. There is a place for them, however, because anything that raises awareness of the risks is probably a good thing.

I am not sure that the messages are necessarily tailored to the most vulnerable types of victims. Frankly, they are inaccessible to some of the potential victims who are most vulnerable. Some thought has to be given

to the right messaging for different audiences, depending on their risks from fraud or from fraudsters.

It is also all very well having messages about what we should be doing with things like passwords—we are advised, for example, not to have simple passwords or to reuse them—but if there was a way in which online providers could enforce that more than they do, that would be helpful, because it would not rely on us as individuals taking action.

In some elements of the public awareness campaigns, I look at the messages and think, "But surely a tech company should be doing that for me, or they can make that happen more easily for me. It shouldn't be down to me". It is a very difficult message to get across. More work needs to be done on the overall strategic communications model on fraud, how we communicate with the public on some of the risks relating to fraud, and how to protect themselves, and, touching on the earlier point, how to report frauds and their consequences. You rightly raise the devastating impact that even a low-volume fraud can have on an individual—the impact on their mental health and their sense of self.

It is a very fine line that we have to tread, but, clearly, more efforts and more effective efforts are needed.

Dr Alice Hutchings: In an ideal world we would have resources that are dedicated to investigating offenders, and we would have platforms being able to stop crime at a very early stage so that these are not necessarily seen by users. Perhaps if these types of approaches were taken, the reliance on consumer awareness and general awareness campaigns would be reduced, particularly as we do not necessarily know how effective these are, and some of the approaches may be more harmful.

Passwords are an excellent example. Passwords are terrible security. The only reason we still use them is because we do not have a usable replacement for them. We used to have a requirement on many platforms—some of my accounts still have this—to change passwords regularly. This leads to really insecure passwords being developed. Some of these things can have unintended consequences as a result, and it is good to be aware of these.

Baroness Taylor of Bolton: Dr Mersinas, you mentioned that you could suggest some interventions that might work and that you might write to us. We would be very interested in that. Do you know who we as Joe Public actually take notice of? Do we take notice of the big public campaigns, or do we take notice of people we recognise on television telling us things? How do we absorb the information?

Dr Konstantinos Mersinas: Let me start first with the fact that the majority of attack vectors or successful breaches and attacks come through social engineering and phishing. That is clearly reported almost everywhere. That is why I insist in a good way on behaviour change.

With regard to the evidence, we asked people across the population whether they knew where to report a number of cybercrimes, and we observed a lot of confusion. You can have two things and they are both not working well. You can either have many campaigns, approaches and organisations offering help, or providing lines and so on, or you can have none, or very few. Both can be not useful, because, on the one hand, information can be toxic and can cause a lot of confusion, and, on the other hand, people do not know who to contact. In general, we saw that people did not know who to contact or how to respond to incidents or problems that they were having.

I want to go back to something that Kathryn mentioned, which is the tailoring. We collected evidence on fraud targeted at the elderly. There is a clear indication that we need to customise the messages in the approaches here, because the elderly can be considered a vulnerable group with regard to different types of fraud and a number of types of fraud. Also, we saw, for example, that they have different perceptions of trust, which was one reason why they tended to fall victim. It is that level of understanding of the targeted groups that we need to have in order to tailor our messages to individuals and groups.

Q68 **Baroness Bowles of Berkhamsted:** I would like to turn now to the current legislative framework and ask whether you think the Fraud Act 2006 and the Computer Misuse Act 1990 are still relevant to the prosecution of contemporary cyber-fraud cases. Does the current legislation need to change to protect the consumers of the future?

I also have a couple of supplementaries that I will give you up front. For example, if you have set up a false networking account, social media account or aliases, there is nothing criminal about that unless you make money out of them. Would it be better if things such as identity theft per se could be stopped? Is that an example of where you might get in earlier and break the chain, or would they not be prosecuted? At the moment, they would not, because there is no loss, but even if it were available, would prosecutors bother?

Another point about the Computer Misuse Act is that some people cite that as meaning that they cannot operate defensive measures. When somebody has been attacked and they need to investigate who is doing the attacking, they themselves are breaching the Act. Are there very many of those counterproductive issues arising from legislation?

Dr Alice Hutchings: I am really surprised at how well the Computer Misuse Act has stood up over time, particularly given the changes in technology since 1990. There have been amendments to take account of things like denial-of-service attacks, and to be consistent with the Budapest convention, but, overall, it has been really quite an interesting piece of legislative history in how relevant it remains.

There are some issues—things like the possession of hacking tools used by penetration testers to test networks, the possession of which is a crime. We have guidelines in the Crown Prosecution Service saying that people will not be prosecuted for their possession, but it creates some

stress for people in those industries that they could be prosecuted. Technically, it is a crime. If there are going to be changes to such legislation, those types of considerations need to be thought about really carefully.

You gave an example of using fraudulent identities. This is something that researchers might do to carry out research to identify how much crime there is, for example. You could be creating legal challenges for researchers. Do you then require a real name policy? On social media this would have very detrimental consequences for some groups of people, for example. Changes to address those issues need to be very carefully thought out.

Kathryn Westmore: Picking up on the Fraud Act, my view is that it remains a pretty good piece of legislation from a fraud perspective. I think it captures most types of fraud, whether they are happening offline or predominantly now online, particularly fraud by misrepresentation. Similar to Dr Hutchings's point, it is hard to imagine what effective changes to the Fraud Act would make a significant impact without having the adverse consequences that Dr Hutchings rightly points to, particularly with regard to something like identity theft. It is very hard to understand or to work out how legislation can best deal with that issue. I know from speaking to a lot of people in the industry that there is a lot of concern about it at the moment as a topic, but I am not sure that the Fraud Act is the place to address those issues.

The issue with the Fraud Act from my perspective rather than the legislation itself is the enforcement and prosecution under the legislation. As we all know, there are limited resources and the cases can be very complex. As we touched on earlier in this discussion, particularly with online fraud, where some of the perpetrators or key figures are based overseas, there are jurisdictional international issues that mean that the Fraud Act will not be relevant. I think that as a piece of legislation it still stands up in its definition of fraud.

Baroness Bowles of Berkhamsted: The big issue is more taking action under it and lack of resources among prosecutors.

Kathryn Westmore: Absolutely. The CPS has a relatively small number of fraud prosecutors. A lot of the cases are quite complicated and complex, and last for a long time. Particularly with some of the frauds that we been talking about today such as volume frauds, it can be hard to justify the cost of the prosecution when the frauds themselves are low value.

Baroness Bowles of Berkhamsted: Is the prosecution complicated because the issues are complicated, or is the prosecution complicated because of the way you have to do it under the Fraud Act? If you have the simple, small scams in high volume, is it merely the high volume that is complex? What makes some of the simpler scams complex from a prosecution perspective?

Kathryn Westmore: From a scam perspective they are relatively simple to explain. Some of the complexity comes in the organisational element of it. We have talked about how they are entrepreneurs and about the number of people involved, the fragmented supply chain of some of the technology and the skills that drive these frauds. Prosecuting a low-level individual fraudster may not be hugely complex, but trying to prosecute the operation of which that low-level fraudster is a part is far more complicated. By picking off the low-hanging fruit of the individual fraudsters you are not necessarily making a huge dent, because the organised groups that sit behind a lot of these frauds have an endless supply of people they are recruiting, and they will just bring in somebody else to replace that person.

For me, the complexity of the prosecutions comes in trying to take down those complicated groups, with many strands, some in the UK and some overseas, which also interact with other criminal groups. Those cases will be incredibly complex and difficult to prosecute, and will take a huge amount of resources, frankly, but those are the kinds of cases that I would like to see prosecuted rather than the individual who has committed some small fraud. Yes, they should clearly face the consequences of their actions, but, at an overall level, prosecuting one individual is not going to make a huge difference.

Baroness Bowles of Berkhamsted: It is like catching the money mule but not getting the corrupt organisation behind it.

Kathryn Westmore: Absolutely, yes. It is exactly the same.

Dr Konstantinos Mersinas: I will add something quickly with regards to the Fraud Act. The definition of fraud by false representation, in my opinion, works very well with social engineering and phishing. It captures the pretexting, as we say—the scenario, the narrative and the story that the attackers build in order to phish, to trick, the victims. I do not think this needs any change, to be honest. As mentioned earlier, we need to work under these things, and perhaps it is a matter of resourcing.

There has been some criticism of the CMA— the Computer Misuse Act. As Alice stated, it has worked well for so long. The one criticism that might have some base is that, in the pure definition of hackers, it is not like the highly skilled hackers that have been prosecuted. We have seen exceptions to this, but the majority of individuals prosecuted under the CMA have been low-skilled criminals, who perhaps failed to do something or failed to take some technical measure and they were found to have unauthorised access, for example. The fact that there is a clear link, and I think it happens all the time, in Section 2 of the CMA with regards to further offences, which is more often than not fraud, allows for a good connection, a good combination, between the Acts. I think we need to work under the Acts, not necessarily changing anything there.

Q69 **Lord Young of Cookham:** Lord Browne half asked my question a few moments ago when he asked whether anyone else was tackling this better than we are. We have heard that this is international and every

other country is facing the same problems that we are. Kathryn told us that we needed a coherent, government-level strategy on cyber-enabled fraud. The question is: is there another country out there, facing the same problems as we are, that has got its act together and has a coherent approach, and is this something that we could learn from? If there are good examples, you can always write to us if we are beginning to run out of time. Alice, do you want to have a go?

Dr Alice Hutchings: I would like to highlight the FBI model, which works closely with industry. It has the National Cyber-Forensics and Training Alliance—the NCFTA. They have police from all around the world, including some from the UK, who go over there and work with them, and the FBI and people from banks and major industry all sit down together and try to address big crime issues in an open way, without many of the problems that you have with collaboration in this space.

That works in a really interesting way. There have been some attempts to replicate that, but there needs to be a level of willingness to engage in this process, a level of openness and willingness to share information, and to collaborate with academia. I have done some work with the NCFTA in the past; I have gone over to Pittsburgh and spent some time with them, and it has been a really eye-opening experience.

Lord Young of Cookham: Does anyone else want to come in, or would you prefer to drop us a line if there are some good examples?

Dr Konstantinos Mersinas: I have just a final comment here, because we have been working with the Metropolitan Police and we have been in touch with other local police departments. There is a lot of effort there and willingness, but it is still a matter of resources and upskilling police officers. One idea that I know has been implemented in other countries to a larger extent is to have specialist civilian staff either working for or collaborating with police departments. Again, I am fully aware of some of the processes that the Metropolitan Police undertake, but it is not easy to prioritise the issues all the time due to the volume or the lack of resources.

The Chair: Thank you all very much indeed. Thank you very much for your time this morning and for answering all our questions. If there is anything else that occurs to you after the session, please feel free to write to us to draw our attention to anything that you feel we should be aware of. I want to thank you all for being here this morning. I know that preparing for a Select Committee is pretty time consuming. We will now suspend the meeting to bring in the next witnesses but thank you all.