Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and Digital Fraud

Thursday 24 February 2022

9.25 am

Watch the meeting

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

Evidence Session No. 1 Virtual Proceeding Questions 1 - 12

Examination of witnesses

Alice Adamson, Euan Neill and Duncan Tessier.

Q1 **The Chair:** Welcome to this evidence session of the Select Committee on the Fraud Act 2006 and Digital Fraud. A transcript of the meeting will be taken and published on the committee website, and you will have the opportunity to make corrections to that transcript where necessary.

I welcome our three witnesses to this first public evidence session of the committee. We are joined by Alice Adamson, who is the director for victims and vulnerability policy at the Ministry of Justice, Euan Neill, who is the head of fraud pursue and law enforcement at the Home Office, and Duncan Tessier, who is director of economic crime at the Home Office.

Members will declare their interests when they ask questions, so let us get under way. I declare my interests as a non-executive director of Santander UK and the Financial Services Compensation Scheme, chair of the Association of British Insurers and a member of the UK advisory board of Grayling.

Thank you again to our witnesses for joining us. I will start with a fairly broad question. From your departmental perspectives, what do you think are the most significant fraud risks facing individuals and businesses? Perhaps you could give a sense of how we have got to this stage; what has allowed fraud to flourish in the UK so that we see these enormous, rather concerning numbers now.

Duncan Tessier: Thank you very much, Chair, and good morning, everyone. On your question about the biggest risks, as you said, we have seen a very concerning rise in fraud over the latest period, and the latest crime stats show a 36% increase in fraud offences, which is 5 million offences. That means that fraud is more than 40% of all recorded crime now, and when you add in cybercrime we are talking about greater than 50%.

The risks are a number of things. We are seeing a growth that is very worrying in what we call authorised fraud, which is growing the fastest of the proportion of fraud. We are seeing a slight increase but more of a plateauing in what we call non-authorised fraud. To be clear, authorised fraud is where the user authorises the fraudster in some way to make the payment. Non-authorised fraud is, for example, credit card theft done without the user's knowledge.

What is worrying about the growth in authorised fraud is that the mental health impacts that go with that kind of offence are greater and more concerning. It also requires a different toolkit to stop, because with non-authorised fraud you can introduce more controls like two-factor authentication and confirmation of payee in the financial sector. That has been successful to some extent over the last period, and I think it is behind the trend of some slowing in the growth of that type of fraud, but in authorised fraud it is down to the user. We know that fraud is a very flexible crime and that they find a way through the weaknesses in the system, so the target becomes the person and playing on the person's emotions and trust to get them to make the payment, which is why it is so concerning.

Your second question was about why we are seeing this big growth. There are a number of macrotrends underneath this but, to state the obvious, one of them is the growth in the use of the internet. That means that more and more citizens are online and are living their lives online, but that opens them up to this cyber-enabled fraud. That is probably the big macro factor.

There is another reason why this is of particularly acute concern in the UK. Looking at international comparisons is not straightforward—the data is very poor internationally—but it seems that there is a particular issue emerging in the UK. Online enablement is greater in the UK, so more people are online in the UK. London is a huge financial centre, which means that there is more money around. The English language is relevant here, because criminal gangs can operate in that language and therefore target the UK.

All those factors probably explain the growth. I am very happy to talk in due course about the Government's approach and response to that.

The Chair: Do not fear. We will ask you questions about that. Thank you. Euan, because of the limited time, I will not ask you and Duncan to answer both questions unless there is anything you particularly want to add. We will have some specific questions for you later.

Euan Neill: To build on the point about fraudsters adapting, over the pandemic we have seen that they have targeted places where people are moving online. With increases in online shopping, auction fraud and romance fraud, they have moved to where people have gone.

The Chair: Yes. We are very interested in how quickly they move, so that will come up as well. Alice, what are the most significant risks, and how have we got to this stage?

Alice Adamson: Thank you, Chair. I do not have an awful lot to add to what Duncan said. The Ministry of Justice is responsible for the legislative framework within which fraud is prosecuted. In our view, the Fraud Act remains an excellent and quite wide-ranging piece of legislation but, of course, we welcome questions from the committee about how it is operating.

The Chair: Yes, and we will have some. Part of the committee's remit is to look very specifically at post-legislative scrutiny of the Fraud Act 2006. Thank you very much for those answers.

Q2 **Viscount Colville of Culross:** Good morning, and thanks very much for coming. What you said about the growth of citizen-authorised fraud was very interesting. How effective are the current anti-fraud policies in combating these highly digitised business models of criminal activity, particularly citizen-authorised fraud? I am also very interested in what can be done to improve ID verification. Can AI and technology be used to try to build up our armoury to stop these online scams?

Duncan Tessier: On the first question, I made a point in my earlier response about the adaptability of this crime type, which is uniquely difficult in this case. We see that we can put in measures that make an impact; I mentioned confirmation of payee, which we believe is one of the key reasons why there has been a real slowdown in the growth of non-authorised fraud like the stealing of credit card details and using those to purchase. That kind of technological innovation can slow things, but then you see a shift into a different area where there is a different weakness, so there is a constant evolution in this space.

More broadly on the question of how effective the current policies are, the key thing is not to think that there is one solution to this. There is no silver bullet. It needs to be an end-to-end, systemic response that enables us to target this growing threat. I mean two things by that. One is that you need to work on what we in the Home Office call "protect policy", which is how you support citizens in protecting themselves against fraud with the right kind of information, but also how you support industry through regulatory frameworks and encouraging partnerships to technology to support themselves.

That is the protect strand. You also have to have a credible "pursue response", as we call it. You have to have the right law enforcement response as well, and I can talk more about that if you want me to. The

key point is that effectiveness is defined by doing all that in an end-to-end way across the huge swathes of our economy that this affects.

Having said all that, I think what you are really getting at is how effective our technology is. We need to do more and we need to do better on this, because clearly what we are doing is not getting hold of the threat enough yet.

You also asked about ID verification. This is part of the protect agenda and is important. It is one component of what needs to be an overarching response. The DCMS is leading some important work on digital ID. It is setting out what it calls a trust framework for how to verify ID, and it will be an important component of our anti-fraud strategy. I should say that there are also risks to that, because you need to make sure that the verified ID is not then exploited by fraudsters who use the fact that it is verified to conduct further fraud. There is a balancing act there and it is not straightforward. I hope that starts to answer your question.

Viscount Colville of Culross: That is very helpful. Euan, can you add to the enforcement component of that and what we can do to try to deal with these highly digitised business models?

Euan Neill: The key here is that the fraud law enforcement system has been underresourced, and we are looking to change that now with our investment under the spending review. As that comes online, the fraud response will link through into the cyber system, which is well established—the national cyber security strategy of 2015 established the first of the cybercrime policing responses—in how we tackle the online component of fraud better.

Viscount Colville of Culross: Alice, do you have anything to add to that? No. Thank you very much.

Q3 **Baroness Bowles of Berkhamsted:** There is a large amount of a cross-departmental nature in tackling fraud. Various different departments are involved. How do you collaborate with teams across departments, how effective is that, and are there ways in which it could be improved? Could you touch on how you co-operate with the devolved Administrations? There is a bit of a difference as to who is responsible for what. In that context, is the Scottish Crime Campus a model that is worth following for England?

Duncan Tessier: You make a very good point about co-operation and collaboration. As this committee and many others have noted, there are an awful lot of departments and agencies involved in this, and I think the Treasury Committee has noticed this recently as well. My view is that the fact that it touches so many departmental interests is not a function of the bureaucracy getting it wrong. It is a function of the hugely widespread nature of the threat. I do not think there is necessarily the simple solution of merging everything. We have to work in effective partnership across those interests, and that requires the right governance

frameworks. It is rather Civil Service of me to say that, but it is important in this case.

I wanted to point out how we are doing that at the moment. The overall economic crime strategy for government is led by two departments, the Treasury and the Home Office. I lead the Home Office part and there is an equivalent director in the Treasury. We report up to two key pieces of governance that oversee the fraud landscape. The overarching governance is the Economic Crime Strategic Board, which is chaired jointly by the Chancellor and the Home Secretary. It is also with the private sector, so we have the CEOs of financial institutions, the Governor of the Bank of England, the head of the FCA, and representatives from other industry groups. We have also just brought in the tech sector, as well as the legal and accountancy sectors, to be represented on that board. DCMS Ministers are also on that board. That is the key overarching governance and how we try to oversee the overall economic crime system.

Specifically on fraud, we have the Joint Fraud Taskforce, which is chaired by the Minister for Security and reports into the Economic Crime Strategic Board. That focuses much more specifically on what I described earlier as the "protect" aspect of our response to fraud, particularly how we are working with industry to design out fraud. That was relaunched with the Minister for Security in October and it is an important forum.

That is our overarching ministerial governance. There is also a lot of programme governance, and detailed forums where we work with industry, which I can set out for you if you want me to but you might not. It is not straightforward and it is not easy to co-ordinate across that system, but I think we have a reasonable approach there.

Baroness Bowles of Berkhamsted: It would be quite helpful if you could send us a chart that shows the different relationships and how they are gone about. Also at a lower level, if you discover that something is happening that is relevant in pensions, what is the paste-across, because presumably techniques will be relevant in other departments?

Duncan Tessier: We have what I described as strategic governance setting out the overall policy frameworks. We have very detailed operational governance. The system leadership for economic crime comes from the National Economic Crime Centre, which we set up just over two years ago. It is based in the National Crime Agency and has the overall operational leadership on economic crime, including on fraud. In response to your specific question, it brings together all the operational partners on the details of pensions fraud or romance fraud.

There are threat leadership groups, operational groups, which the National Economic Crime Centre oversees. Those bring together the relevant operational leads in the public and the private sectors, the tech sector, the financial sector, and they share intelligence and information at an operational level to respond to new and emerging threats, to different

typologies of fraud. We have seen some real success with some of those groups.

All of this is developing and expanding, and ways of working are having to improve as the threat evolves, for example in particular bringing in the tech sector, which three or four years ago was not such a focus on the fraud agenda and now very much is. We are having to advance those partnerships operationally and strategically to bring in the new sectors. I hope that covers your question.

Baroness Bowles of Berkhamsted: What percentage of its attention is given to fraud? Is it 40%, which reflects the amount of fraud within crime?

Duncan Tessier: Which specifically? As in the economic—

Baroness Bowles of Berkhamsted: In the National Economic Crime Centre.

Duncan Tessier: It is a huge focus and a growing concern. If anything, it is probably one of the top priorities for the National Economic Crime Centre at the moment, given the growth rates that we set out at the start of the hearing. It is a very big focus for the NCA and, as Euan commented earlier, the spending review has set out an important uplift for our response to economic crime and fraud. The big focus now, including for the NCA, is how we build up our law enforcement capacity to respond to the fraud threat. We have set out £400 million of new money for economic crime over the next three years in the spending review, of which £100 million will be for our fraud response.

Baroness Bowles of Berkhamsted: How does that liaise with the devolved Administrations?

Duncan Tessier: Euan might want to talk to the detail of that. Euan, do you want to come in on that point?

Euan Neill: The devolved Administrations work in various different ways. England, Wales and Northern Ireland all work through the central City of London Police Action Fraud system. Police Scotland has its own reporting system for fraud or you report directly into Police Scotland, but we work very closely with Police Scotland. It is involved in most of the working groups at the operational level and the NCA has a UK-wide remit, so it is tackling fraud across the UK. We are just starting to work with the devolved Administrations on the strategy. The new approach we are taking is tackling fraud as we spend this money and so we are establishing the relationships and working out where their priorities are and where we can work together.

Baroness Bowles of Berkhamsted: Thank you. Alice, do you have anything to add? Do you learn from what happens in the different legal system in Scotland?

Alice Adamson: Not particularly at my end of the criminal justice system. We usually tie into the governance that the Home Office pulls together to help co-ordinate across Whitehall. We also have a separate interest at the far end of the CJS in how the courts are dealing with fraud. We have regular liaison with the Serious Fraud Office, the Attorney General's Office and the CPS, but those are specific to England and Wales, given the nature of the MoJ's remit in that space.

Q4 **Baroness Henig:** Good morning, all. First, I will declare my interests. I am non-executive chair of a private security company, SecuriGroup, which is based in Glasgow. I also chair the Certified Security Professionals Registration Authority and I am president of the Security Institute.

I will direct my question to Euan first. I am particularly interested in the theme of collaboration with wider non-governmental departments and agencies, and there is a whole raft of bodies out there, all pursuing crime. I will select two at random: the City of London Police and HM Revenue and Customs. Both those bodies have had huge fraud operations in the last few years. They have done investigations and all sorts of things. How do you liaise with them and how do you draw on their experiences? How is the knowledge and expertise that is gained pooled across all departments?

Euan Neill: The City of London Police are the national lead force for fraud. They run the Action Fraud and National Fraud Intelligence Bureau systems, for which we provide the funding. We work very closely with the City of London. It is a core part of the response. It works very closely with the National Economic Crime Centre, which Duncan talked about. The way the operational governance works, the NECC and the NCA lead the national picture and work across all the sectors and organisations.

When it comes to policing, we work very much through the City of London Police, which will help to build the capacity within policing and to spend the spending review money that we talked about. It gathers information and knowledge from victims through Action Fraud; we ask people to report fraud to Action Fraud. The information we get from that is insightful and helpful to our response. A lot of the numbers that Duncan and I have talked about have come from Action Fraud and from that reporting. They have relationships that work on particular types of fraud, and they work on communications, so they often lead a lot of the campaigns on particular events. They provide advice to victims of romance fraud on Valentine's Day, and on holiday booking in November/December, when people book their holidays. We do not just draw on their knowledge; we are very keen that they take action. It is an integral part of our response.

When the Home Office talks about fraud, it is talking about fraud against individuals and businesses. HMRC's main responsibility is fraud against the Exchequer. There are lessons that we can learn from that, and we work quite closely on issues where its brands are being used and people are being convinced that they are being rung up by HMRC. We work

closely with it to make sure that there is protection and advice in place to stop people falling victim to that.

On the more practical capabilities, the NCA and HMRC work closely together at a national level to share capability. Drawing on the lessons they learn, we have to be a bit careful, in that HMRC has a lot more direct ability to prevent fraud, in that it runs the systems, than the Home Office or law enforcement do. We can take some of the learning from HMRC and work with the banks or the private sector, but it is not necessarily as directly applicable as, for example, what we get through City of London Police.

Baroness Henig: It is the collaboration aspect that interests me. The word "underresourced" came up, and "building up capacity". I am assuming that in the governance that you are operating in you do not have that many people working on these issues. Can you give me some idea of the scale of operations in, say, in the Home Office or in your particular areas? How many people are we talking about?

Duncan Tessier: If the question is operationally how many people in the system are working on fraud against citizens and businesses, broadly speaking there are around 1,000 officers in the policing system working distinctly on fraud. That is an idea of scale. If you are talking about the officials in the Home Office, we have a fraud policy unit, which is one of the areas within my directorate, but we also work with a lot of teams across Whitehall. I hope that gives you a sense of it.

The other point in this context is that we are looking to expand the operational footprint of working on fraud because of the growing threat, which is why the spending review money has been made available. We will be looking to put hundreds of new officers in place over the next three years. We are also increasing the input from the intelligence agencies on the response to fraud, which is a significant development. It has been in place for a number of years, but this is about starting to step that up, which also came out of the new cybersecurity strategy that we published last year. We have the National Cyber Security Centre, which has some high-end capabilities that are being deployed increasingly towards the fraud threat as well.

Q5 **Lord Vaux of Harrowden:** Good morning. First, to declare my interests, I am a member of the Institute of Chartered Accountants in England and Wales and I have a shareholding in Fidelity National Information Services Inc, which owns Worldpay among other things.

I have a couple of questions. The first is for Alice Adamson and Euan Neill. How do your departments engage with external stakeholders such as consumer groups, industry bodies and victims when designing and implementing policy? I am particularly interested in industry groups such as telecoms, finance and tech, and I am interested to know whether you feel you are getting the appropriate levels of engagement from those groups.

Alice Adamson: Perhaps I might answer that question first, because the MoJ has a slightly more limited interest, given our responsibility for the legislative framework. We last did post-legislative scrutiny on the Act in 2012, and we took a range of evidence on the Act at that point. The committee has asked us to have another look at the Act and we may get into more detailed questions on it. We will be engaging widely to make sure that we understand whether the Act is still delivering in the way it should be.

Noble Lords may be aware that we have just run a victims' Bill consultation, which closed on 3 February. It was across victims of any type of crime. We did not have any specific responses just on victims of fraud. I do not know whether that is because fraud victims do not come together in quite the same way as interest groups for other offence types. Euan might want to talk a bit about how the Home Office engages victims where there is quite a specific programme.

Euan Neill: On the first question about engaging with industry, as Duncan said the governance we have is public/private. That grew out of the economic crime plan that was launched a couple of years ago, which is a joint industry and government plan to tackle economic crime. How we work with particular industries and sectors varies between working on what we can achieve voluntarily and what we can achieve through more legislative means.

As examples of that, we have launched sector charters with the telecommunications, finance and accountancy sectors, which have agreed a series of joint collective actions to tackle fraud. At the same time we are engaging with the tech sector in the process of agreeing what more it could do. We are also introducing the Online Safety Bill through Parliament, which now includes fraud as one of the crimes within its scope. We are taking a range of approaches. We are mostly trying to work collaboratively, but where we feel the need there is the opportunity for legislation.

We work very closely with victims through the City of London Police. Victims present most often to the police, and there is an economic crime victim care unit in the City of London Police specifically to engage and support the most vulnerable victims, but all victims who report fraud to Action Fraud will receive some support. We also have put a victims' working group in place with the Serious Fraud Office, where we are working with the main victim organisations to better understand what we can do to support victims.

Lord Vaux of Harrowden: On the industry side, are there areas where you do not feel you are getting the right level of engagement and reaction from industry?

Euan Neill: I might let Duncan answer that one.

Duncan Tessier: I am very happy to respond on that. I think the industry response has been very strong in these areas. As I said, the

overall strategic governance on this agenda is through the Economic Crime Strategic Board, which has key representatives from the financial sector, the telco sector and now the tech sector. I think we are working very collaboratively. In the finance sector, for example, there are extremely strong interests to try to reduce fraud because it is very costly for that sector, with over £1 billion in losses. We are happy with the level of collaboration, but there is no doubt that we need to go further across all those industries and more broadly. We will be looking for collaboration and support with those sectors to do that.

Q6 **Lord Vaux of Harrowden:** I could go on for ever, but I know that we do not have much time, so I will move on to my second question, which is for all three of you. I think that the resignation of Lord Agnew highlighted the level of fraud associated with the Covid-19 support schemes. I am interested to hear how your departments have been seeking to tackle that sort of fraud and how successful you feel that has been and is being.

Duncan Tessier: It is clearly a very important issue. I will steer your attention to the distinction between what the Home Office does and what other parts of government do on this agenda. The Home Office leads the Government's response to fraud against citizens and businesses. The Cabinet Office leads the response to fraud against the public sector, which is largely what I think Lord Agnew was referring to. I think it is best that you direct those questions to the Cabinet Office, which I am sure will come into your inquiries later.

Lord Vaux of Harrowden: Thank you. Alice, do you have anything to add to that from the Ministry of Justice side?

Alice Adamson: I am sure noble Lords will be aware that the Justice Committee has published a report on Covid and the criminal law. We are due to respond to that report soon. I do not feel able to prejudge what the report will say, but you may want to take it into account as part of your evidence for this inquiry.

The Chair: Yes, thank you. We are very aware and conscious of not treading on too many toes. Baroness Bowles, I think we need to go back so you can declare your interests.

Baroness Bowles of Berkhamsted: Yes, I am sorry. I think that I have to declare that I am non-executive director of the London Stock Exchange and of Valloop Holdings Ltd.

The Chair: Duncan, I want to follow up on one answer about the Covid-19 fraud. Given the Home Office expertise, did the Cabinet Office or anybody else like BEIS ask the Home Office what they might need to do to be cognisant and to able to chase down fraud in the Covid-19 schemes?

Duncan Tessier: There was a lot of collaboration, and the National Crime Agency has a remit to target serious organised crime in that capacity where there is organised criminality behind, for example, the bounce-back loan frauds. I know that the NCA was sharing intelligence

and using some of its capabilities to support other departments in that respect. Yes, that collaboration was happening, and the Home Office was represented on overall governance. There was join-up there.

Q7 **Lord Young of Cookham:** Good morning. Can we go back to the issue of resources, which was touched on? I think in an earlier exchange Euan said that this area was underresourced at the moment. With 42% of crime against the individual being fraud and only 1% of police resources, it seems at first sight to be a most heroic mismatch. When you drill down into the 1% of police resources that are devoted to fraud, you find, as we discovered last week, that at the local level the police simply do not have the portfolio skills that you need to tackle the sorts of fraud that they were confronted with. We were told about the uplift in the spending review, but even after that uplift the Treasury Committee still said, "Economic crime seems not to be a priority for law enforcement".

What is your response to what the Select Committee has said and to what, despite the uplift, seems to be an extraordinary mismatch between the volume of crime and the volume of resources, as I said?

Duncan Tessier: The critique that there is underresource in the system has been made by a number of independent reports, including most recently the policing inspectorate report on the fraud system, and, as you say, the Treasury Select Committee pointed to it. I refer you to the remarks that the Minister for Security made at the Treasury Committee where he accepted that we need to do more on fraud, and the Government's beating crime plan, published last year, says that. There is a recognition that we have to go further on fraud.

The spending review sets out an uplift as a response to that. Historically this area has not been as invested in as other crime types, but we are seeing a substantive increase in funding of £400 million in the economic crime agenda over the next three years. That will come from a new levy proposition that is now being legislated for. It will be a levy on the private regulated sector that pays for economic crime capability. I raise that, because it is not just about funding but about sustainable funding, and the point about the levy is that you have a ring-fenced £100 million a year that can go into supporting economic crime capability. Within that £400 million over the next three years, £100 million is on fraud. That will pay for a step up in the law enforcement capability.

You mentioned local forces. Importantly, the focus of that investment will be at the national and regional levels, because the view is that increasingly fraud is a transnational and a national threat. That does not mean that there is not a very important role for local policing. There is, but it needs to be supplemented and supported by the enhancement of national capability. I think that will drive an important shift particularly in understanding the intelligence picture so that we can go after the largest organised crime groups who are driving this. That requires investment in intelligence officers in the centre, in the NCA, where they have access to the highest-end capabilities and across the connection into the

intelligence agencies. My point is about having the investment in the right place to drive bigger steps forward.

You are absolutely right that we need to take strides forward in our law enforcement response, but it cannot just be about your law enforcement response. I commented in my opening remarks on the need for a real end-to-end systemic response to fraud. An oft-quoted phrase is, "You cannot arrest your way out of the fraud pandemic", and I think that is absolutely right. The protect measures that I alluded to earlier are absolutely critical, so we need to work on our communications campaigns to help citizens to support themselves, and we need to work with industry to design these frauds out of the system, particularly in the tech sector.

The Online Safety Bill has been mentioned, but it is also about what we can do with the financial sector and the telco sector. Those things can reduce the flow into the system, but we also need to have the appropriate deterrents. The investment in law enforcement that I alluded to is important, as is the bringing in of the intelligence agencies and cybersecurity skills.

We have to drive an end-to-end response, and the Government will set that overall response more fully later in the year through a fraud strategy. However, we have already published the approach to that. In the beating crime plan and in the economic crime plan statement of progress, we have set out the framework that we are now building on through the fraud strategy later in the year. I hope that is clear.

Lord Young of Cookham: Post the uplift, what percentage will be devoted to fraud instead of the current 1%? You may want to drop me a line about that.

Duncan Tessier: Yes, I am happy to do that.

The Chair: We now move to the Fraud Act itself.

Q8 **Lord Browne of Ladyton:** This is your moment, Alice. Helpfully in your first contribution you expressed your view that the Act remains relevant and sufficient, so let us test that. I think it is only fair to you that I give you some sort of indication of the key concerns about the Act that we have already heard from others. I am sure you are aware of them, but I will just list a few of them to concentrate your mind. When you are responding to this question, maybe you could address the issue of continued relevance, particularly in an environment in which digital banking and payments have grown exponentially since 2006.

Has this Act had any impact on changing and increasing unprosecuted fraud? That is against a background of over 5 million cases a year, of which a minuscule amount gets anywhere near the courts. I have no idea how many of these judicial outcomes have convictions, but a very small number of them—about 6,000, by my calculation—have judicial outcomes. It is not a great deterrent. Does the maximum sentence continue to be adequate, given the impact this is having on the country? Finally, is prosecuting corporate criminal liability too complicated to do in

the framework that we have? The floor is yours.

Alice Adamson: Thank you. That is a very wide-ranging question, so please come back to me if there are parts of it that I do not answer up front.

On continued relevance, the post-legislative scrutiny that took place in 2012—admittedly that was 10 years ago, and I understand why the committee is interested in the relevance of the Act, given the passage of time—showed that because the Act is quite wide-ranging and simplifies the law, it has allowed for prosecution of quite a wide range of offences in emerging technologies. Those technologies have changed, but a lot were things like credit card fraud, PIN-enabled fraud, so a technological element was considered at the time. As I referred to earlier, of course we are very happy to work on the memorandum that the committee has requested, and we will do a post-legislative exercise of part of that to make sure that the issues that you have raised are covered.

Interestingly, you said that I would be aware of concerns that have been raised. The department has not had any evidence that the Fraud Act is not doing what it needs to do, so if the committee has evidence that it is willing to share with us, whether at publication or beforehand, we would be very interested in seeing that and being able to consider it.

Based on the evidence that we have seen, I do not think that the Act itself is a reason for unprosecuted fraud increasing. Certainly in our on-going conversations with the CPS, the Serious Fraud Office and the Attorney General's Office, who I believe may be coming to talk to the committee at some point in the future, we have not had evidence from them that the Act is in any way stopping them bringing forward prosecutions, or indeed successfully prosecuting. Of course, fraud prosecutions are incredibly complex, and cases take a very long time to go through the system because of the level of complexity. There are often multiple defendants in a case. I do not think that element of the challenge that the prosecutors are facing relates directly to the legislative framework that underpins the prosecutions that they are bringing forward.

On the maximum sentence, I think we believe that it is still appropriate, but, again, if there is evidence to the contrary, we would welcome sight of that.

Finally, you asked about corporate criminal liability. As noble Lords will be aware, the Government did a review of corporate criminal liability in 2017 and the evidence we heard was inconclusive, which made it quite difficult to agree a route forward. We have a project with the Law Commission at the moment looking at the question of corporate criminal liability, and it is due to report to us in the spring. We hope that that will help to provide clarity on the way forward, because we recognise that that is quite a complex issue in a very complex area of law.

Lord Browne of Ladyton: Perhaps I should have been much more

specific with my language, to be fair to you, Alice. These issues come from the briefings that we have received rather than evidence that we have had, although we will go looking for the evidence to support what is already out there in open source. This information is available in open source. It is not particularly from evidence that we have received, but I think we will look for the evidence to support it.

As with the amount of resource earmarked to deal with this challenge, there is an extraordinary disproportion between the number of crimes or offences that have been committed and the number that result in successful prosecutions in our criminal justice system, no matter how complex the infrastructure is. It is clearly part of our job to try to see why that is the case and to make recommendations, helped by you and others, to improve that.

Do you share the concern that the vast criminal justice system that we have in this country, with all its resources, is having such a minuscule effect on something that affects so many people?

Alice Adamson: As Duncan said earlier, absolutely we agree that more needs to be done. For me, an important consideration is whether the Act itself is in any way stopping the number of prosecutions going through the system. A lot of what is required is the investment in making sure that the right resources are available to the police and the prosecuting authorities. Then, of course, we in the Ministry of Justice have the responsibility to make sure that there is also the capacity and the expertise in the court system to take the cases through. So, yes, we should do more. I agree with that point.

The Chair: Thank you. Of course, we will publish the report and the evidence eventually, and hopefully people responding to our call for evidence will share their thoughts on the Act.

Q9 **Viscount Colville of Culross:** I want to ask about the Computer Misuse Act. We heard from CIFAS that it thinks that the Act is out of date and does not reflect the risks posed by cybercrime today, especially the danger of being hacked. The Government have announced a review into this Act. What is your assessment of the Act as it relates to policy-making on digital fraud?

Duncan Tessier: Our immediate view is that the Act is fundamentally not working. Given that the Computer Misuse Act was from 1990, it has been surprisingly resilient to the enormous technological shifts, I think because it is quite broadly scoped and has therefore been quite flexible and able to adapt to the growth and change in technology. Having said that, it is clearly absolutely right that we look at it again. I think that is why the Home Secretary announced in May 2021 that we were going to have a call for evidence and do a further review of it, and some of the issues that you raised are part of that review.

There has been a call for evidence, and we have had some key themes coming out of that in the fraud space. One area that particularly the

police have pointed out is taking down domain names that might be fraudulent or used for other malign purposes, so that is being looked at. In response to the call for the evidence, there were calls to consider whether there should be a strengthening of a cyber duty to protect, so you ask firms to bake in cybersecurity controls as a matter of legal principle. That is an idea that has been put forward and will need to be considered. If the committee has detailed views and thoughts on this, they would be very welcome by the Home Office as part of its process. Euan, do you want to add anything more on this?

Euan Neill: The only thing I would add is that that will also look at the powers that law enforcement needs on the seizing and retention of data in order to prosecute those offences.

Viscount Colville of Culross: Duncan, you did not reply to my question about hacking. Do you think that the Act is responding well to the increase in hacking into computers that we are seeing?

Duncan Tessier: It has not been specifically raised with me that that is a big issue. Euan is the expert in this area. Euan, do you want to speak to the hacking point?

Euan Neill: The Act itself is, as Duncan said, very broad. It deals fundamentally with unauthorised access into a computer system to retrieve data, which is hacking. As a piece of legislation, that still accords with the criminal activity that is being undertaken. Part of the review is whether we have all the powers we need to prove that, and it covers all the things that are being done. At core, however, the Act covers the hacking.

Duncan Tessier: The issue that has been raised with me specifically on hacking is more about ethical hacking, for want of a better word. That is where businesses need to retrofit and check whether their systems are defended. There are concerns that that could be a Computer Misuse Act offence. It is a technical area and it is quite a tricky one, so that area that has been raised with us, but it is not straightforward.

Viscount Colville of Culross: Duncan, when do you think you will have some results from this review that you can share with us?

Duncan Tessier: I do not think that the Government have set out a timeline yet for when they will respond, but I know that the consultations and deliberations are occurring, and we will set out the results in due course.

Viscount Colville of Culross: Alice, do you have anything to add to that? No. Thanks very much.

Q10 **Lord Sandhurst:** I do not believe that I have any interests to declare. I will look at this in two ways. The first is from the legislative angle. I will direct this question to all of you, but Alice might want to go first, unless one of you thinks that you are stronger on it. That is to set you up.

We have heard about protect measures end to end. What in your opinions is the most effective means of tackling fraud? Do we need more laws or different laws, or simply better implementation of what we have? Should we be doing more to enhance consumer campaigns, and can we do more with regulators? Over to you. I should say that after that I will be asking about the providers—in other words, fintech, financial services and so on—so focus on the legislative side.

Duncan Tessier: I think the answer is that absolutely we need to do more on the protect side, including through legislation. Some of that has the capacity to have a transformative effect, albeit, as I said earlier, that there is no one silver bullet here and we need to push across a number of dimensions at the same time in a number of sectors. As has already been referenced, the Online Safety Bill is a very important step forward with its inclusion of fraud, and that speaks directly to your question.

We also need to look at regulatory legislative options in other sectors, where appropriate, as well as at voluntary action. As I mentioned, the financial sector is key. Innovations like confirmation of payee have been very important, and moving towards two-factor authentication is very important. If there are other regulatory legislative proposals in that space, particularly on information sharing within the sector but also between sectors, the Government are keen to look at those and address them where appropriate. The third sector is the telecoms sector, where there are opportunities to work with industry to do more in the protect space—scanned text messages and scanned calls, for example, are an area that Ofcom has been very focused on and working on closely with industry. There are important tech steps that can be taken there.

Your other question was about the public and information campaigns, and I agree with you again that the other plank of our strategy within the protect pillar is how industry can protect itself but also how citizens can. As part of the spending review money that we have alluded to, we have set up a new unit in the National Economic Crime Centre to co-ordinate the communications to citizens. As we have discussed, there is an enormous number of agencies, both public and private sector, putting out a number of different messages to citizens, and we think we can do more to bring them together, get a coherence to them and potentially issue new communications. It is a key plank of the strategy.

Euan Neill: On the additional legislative side of things, law enforcement also has access to a range of other powers that it can use on fraud. That includes the civil proceeds of crime powers, typically on money laundering or the possession of assets of criminal origin. That is quite useful in fraud, because when someone has a large amount of money in their bank account and they cannot explain exactly where it came from because it came from fraud, it is quite possible to take a lot of money off fraudsters when you can identify it in the right account.

The other side of things is serious crime prevention orders. There are also ways in which we can impose restrictions on serious criminals' activities

under serious crime prevention orders, before and after conviction, and they can be and are used for fraud.

Q11 **Viscount Colville of Culross:** Does Alice have anything? No. Duncan suggested that there might be other sectors. We will park online safety, because we know about that. Are there any other areas where you are looking at new regulations or feel that you may need them? Do any specific areas spring to mind?

Duncan Tessier: I am not sure whether it is regulation or voluntary action or whether it is both together. I mentioned the three key sectors, but there is also an on-going dialogue with the accountancy sector and the legal sector in particular about what more we can do on fraud. The key focus is the financial sector, the tech sector and the telecom sector. The Government are open to propositions on new legislation or regulation across all those, when that is appropriate, but we are consulting with industry on that.

I want to add a point about legislation, because we have not mentioned in this discussion so far the growing threat of cryptocurrencies in money laundering. There are no doubt real positives for financial innovation associated with crypto, but there is also risk, as we see. It is a money laundering issue, but it strongly overlaps with the fraud agenda. Particular legislation that we are keen to introduce in that space is on the ability to seize crypto assets using civil recovery powers. At the moment, our ability to seize is limited to criminal powers. That is an important proposition that we are looking to take forward when legislative time allows, so I wanted to add that.

Viscount Colville of Culross: It is interesting that you mentioned that, because there was a story in the *Times* last week about a cryptocurrency scam. The reporters had spotted this pop-up outfit and followed it through with Companies House and the FCA, but rather drew a blank with those. They did not get anywhere with the City of London either, because they say that the City of London will intervene with the Action Fraud line only when somebody has actually suffered loss, which seems a bit late. In other words, if one of these companies is popping up with some chap living in Pakistan who has a whole lot that is purportedly based in Eaton Square but is not in fact there, there needs to be a means to knock that on the head, does there not? This is part of your Companies House reform, I think.

Duncan Tessier: It is a really good point. As we discussed, we see the broadening out of this agenda and how there are so many linkages. The Companies House reform, the register of overseas beneficial ownership and information-sharing powers are all important underpinnings for an overall economic crime response and response to fraud. Those proposals are important.

On your specific point, I cannot speak to the individual case, but you make a valid point about the importance of proactive law enforcement intervention. Coming back to my point about the additional resourcing,

the focus on centralised cases in the NCA and increasing regional organised crime units in the City of London will also be about having a step towards more proactive enforcement here.

Q12 **Baroness Taylor of Bolton:** I have to declare an interest as a non-executive director of Thales, which is a defence and security aerospace company.

Duncan, it is clear from all that we have heard that fraud is big business for criminals, but the sectors in which they are operating are big business for UK plc. When it comes to regulation across the board, there are some people who think that further regulation would be very onerous and would detract from the companies' success. We are seeing this a little with the online security Bill; some people are saying that Ofcom will be overwhelmed if we do too much here, there or anywhere. Yet at the end of the day our purpose is to try to protect individuals. Do you have a take on how we get the balance of not hampering industry and these sectors too much but giving the protection that is necessary?

Duncan Tessier: You have articulated that there can be a trade-off, and that is the balance that the Government have to strike. However, there is not always a trade-off. In some cases, industry can welcome regulation where it ensures a level playing field or ensures that firms that want to go further are not competitively disadvantaged because a level playing field has been set by government. I refer back to my earlier comments on this point. We know some of the key sectors where fraud is a big risk and we are working closely with them. We have decent strategic governance. We are developing operational governance where we are working closely with these sectors, challenging them and working with them in partnership to say, "Where can we go further? Where might regulation be appropriate?". We are considering that action as well. It is absolutely the right question to ask.

As I said, the macro point on all this is that you cannot arrest your way out of this issue. Protection is the key aspect, so these types of responses will need to be part of our strategy.

Baroness Taylor of Bolton: But each of these sectors is regulated in silos. What is happening in one may not be transferable to another. If we do something extra in the Online Safety Bill, which I hope we will, another silo here might say, "There is a problem for us as well". That is a difficult issue in making sure that it is totally comprehensive. We are not dealing with one comprehensive sector, so it needs to go in at different levels.

Duncan Tessier: A very challenging thing about this agenda is the sheer scope of it, and the fact that the amount of the economy, and firms within the economy, that is touched is so large. We are not dealing with one regulatory regime here. There is a regulated sector for money laundering. There is something that you can put a ring around and say, "This is how we are approaching this". That is not so easy to do for fraud, because it crosses so many different sectors and different legislative

regimes that you might be looking to amend, which makes it more challenging. I think you have made a good point there.

The Chair: I thank our witnesses very much. Is there any final one recommendation or one final thought that we have not asked you about but you came with a burning desire to tell the committee? I think we have winkled out of you, Duncan, your desire for regulation of cryptos, and that is very helpful. Euan or Alice, is there anything finally before we close the session? No.

Thank you all very much. I know that preparing for a Select Committee takes an enormous amount of work, so we are very grateful for your time this morning. Thanks to my colleagues for their discipline in asking questions, and for the benefit of the broadcasters I will say that I now formally end the meeting. Thank you.