Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 23 June 2022

10.50 am

Watch the meeting

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

Evidence Session No. 23 Heard in Public Questions 241 - 249

Witness

I: Max Hill QC, Director of Public Prosecutions, Crown Prosecution Service.

Examination of witness

Max Hill.

The Chair: Good morning and welcome to today's second evidence session of the Fraud Act 2006 and Digital Fraud Committee. A transcript of the meeting will be taken and it will be published on the committee's website. You will have the opportunity to make corrections to the transcript where necessary. We are very grateful to our witness this morning, Max Hill QC, Director of Public Prosecutions at the Crown Prosecution Service. Thank you very much and welcome.

Q241 **Lord Vaux of Harrowden:** Thank you. Mr Hill, could I start with a general question? What is the role of the CPS in tackling fraud? Could you outline the priorities of your new serious economic, organised crime and international directorate and explain how it collaborates with other law enforcement bodies as well as with the Government and the private sector in tackling fraud?

As an additional general question, fraud has ballooned to be the single biggest crime these days, but at the same time the number of

prosecutions has fallen away in the opposite direction. If you could give at a very high level, because we will explore these things in more detail, the main reasons why that has happened, it would be helpful.

Max Hill: Thank you very much for inviting me today. Can I try to address this as crisply as I can? The Crown Prosecution Service across England and Wales is here to provide a prosecution service for all crime types, with fraud and economic crime being one of the significant divisions within our structure. By the time I arrived in 2018, the Specialist Fraud Division of the CPS had created three regional hubs across England and Wales as a way of trying to brigade our resources, because we can all recognise that fraud does not identify country boundaries, or even international boundaries.

As a development of that, on 1 April this year we further brought together our specialists nationwide into the Serious Economic, Organised Crime and International Directorate (SEOCID). That badging tells you that we are here to play a part in addressing fraud, which, as you rightly said, costs eye-watering sums to the country on an annual basis—a figure of some £4.7 billion in the latest captured year. I emphasise that it is only a part.

The guiding principles for SEOCID, the new division—by the way, it has not come at any public expense; we have simply internally organised our resources—are: to develop and share our skills to ensure that the casework tools we use are as efficient as possible and that we are as timely as possible in this very important area of crime; to work with partners; and, crucially, to make sure that we provide the best service that we can to victims of fraud, of whom there are many thousands in this area.

You talked about falling volumes. You are absolutely right that in very recent times the volume of prosecutions coming before court has fallen. Having said that, at the Crown Prosecution Service, because we are just one integral part, I would identify the fall as due in part to the pandemic. I can see in the figures, looking across the last two or three years, that there has been, I would say, an understandable drop-off in cases capable of being brought to court because of the national pandemic that we have been through.

I go from that to another point. As the complexity of fraud increases, the means of fraud increase, and cyber-enabled fraud in particular, is growing with every year that passes. We are bringing cases now, for example, that include what is known as text scamming, involving so-called romance fraud. I could give many other examples that are cyber-enabled. They pop up all the time. It is an ever-increasing task for investigators—we are not an investigator—to try to get to grips with, and to bring the results of investigation to us as early as possible so that we can help shape that within existing legislation and try to bring cases to court.

I would like to come on to one or two thoughts about how we could now look again at the legislation and perhaps fill in some of the gaps that still exist.

Lord Vaux of Harrowden: Thank you. I am sure we will come to those points later. I am interested in the fact that you blame the pandemic. I am looking at a graph that shows, in very round numbers, that in 2010 there were 20,000 prosecutions, in 2017 it was in excess of 10,000, and in 2020 there were 5,000. It has dropped away fairly consistently over time, from the graph I can see. You mentioned complexity. Is it a blockage at CPS level, or is it a blockage in things coming to you that you can deal with? Are there any high-level reasons?

Max Hill: At a high level, obviously on behalf of the Crown Prosecution Service I have to say that it is very important that we are sufficiently resourced to do what we are trying to do. From the spending round in 2021, for the first time some additional resources are flowing in and we will use those right across our headcount to try to improve and be more available.

A phrase that I have not been using very recently, although it is still true at a high level, is that we are a demand-led organisation. The job of the prosecutor is to try to stay ahead of the curve in terms of what police and other investigators are able to put into resourcing fraud investigations so that we are ready for those cases. For issues that are beyond my remit, we have seen fluctuations, shall I say, in the volume of investigative product that is coming to us and in the way it is coming to us.

Having said that, we are seeing some new entities come on board that undoubtedly are helping. The National Economic Crime Centre, sitting within the NCA, is a powerful lever that is helping to look at crime trends, and to encourage investigators nationwide to bring cases forward. We have to play our part in being available through legal advice. We do not give investigative advice; that is for investigators. We are here to identify the elements of legislation that are available, helping investigators to shape what they are doing and build those cases into prosecutions.

The final thing at high level is that the complexity, which I touched on before, is a real phenomenon. You mentioned the period from 2010. You are right that volumes have fallen, but it is in that period that we have all bought iPhones, we are all using digital tablets that have eye-watering capacity, and we are seeing cases with quite extraordinary volumes of material for investigators and prosecutors to look at. We had a recent case, which I think came through HMRC, one of the principal investigators, with 175 digital media items—not files, but items; computers, phones and SIM cards from phones. There were 28 million files that needed to be looked at and gone through in order to shape the case. That digital explosion, as I sometimes refer to it, has had a significant impact.

I emphasise that this is not the fault of investigators; it is a surge in what they have to go through to create an investigation, give it some shape and then, with our help, push it through into court.

Lord Vaux of Harrowden: Thank you. On collaboration with other agencies, how does the CPS collaborate with government in trying to shape policy to improve the situation?

Max Hill: We have a strategy and policy directorate at the CPS and our policy profession is available to sit down with policy teams at the Ministry of Justice and at the Home Office. That is where we principally interact. It is they, not us, who deal with government policy, and it is they, not us, who are legislators, bringing Bills, et cetera, to Parliament.

I hope I am appropriately careful to stay within our remit. We do not campaign; it is not for us to set government policy. We simply make practical the impact of legislation as it changes over time. Where we can help is by giving real-life examples of the difficulties that we face and sometimes the limitations in the way Parliament, with best intentions, has legislated, and perhaps suggest ways in which we can fill in the gaps. That is the interaction.

On the investigative side, which is so important, through secondment and sitting on management and other board structures we have a very valuable relationship with the National Crime Agency and with the NECC - the National Economic Crime Centre – which I mentioned before. We work very closely with them to try to keep on top of what they are bringing forward.

The Chair: Thank you, Director. In those answers you have touched on a number of issues that we would like to come to in more detail. Let us turn to legislation first.

Q242 **Baroness Kingsmill:** There is an opportunity for you to influence legislation now by helping us to form our views about the existing tools. What is your opinion of the Fraud Act 2006, which is our principal interest at the moment, as you see from the title of the inquiry? How useful is it, as far as you are concerned? Is there a wider range of offences that you would like to see added, in particular in relation to all the new crypto stuff?

Max Hill: My view is that the 2006 Fraud Act is a testament to the Law Commission, as later recognised by Parliament, in creating a very helpful new template, bringing together a number of the key fraud offences under one umbrella. We are talking about dishonesty, and essentially all fraud contains elements and aspects of dishonesty, so the model the Fraud Act provides has been extremely useful. Abuse of position of trust as a definition of one of the key species of fraud has been very useful. Speaking, I think, for our team, the 2006 legislation does not present problems. It creates answers and it has been a very useful tool, but it does not stand alone.

You mentioned crypto. It is pretty much fit for purpose where crypto currency offences and certain types of cyber-enabled offences are just species of dishonesty. The template the 2006 Act created is good for that. It is more about investigative learning and legal learning on how we can understand what first appears very complex and very alien, and put that into the straitjacket of the Act.

In this area, as in so many others, there is not just one statute that we look to or use. Very often, when accumulating charges or drawing an indictment, we look beyond or alongside the Fraud Act. We still use the Theft Act for any number of deception-based offences. In the corporate sphere, we have two good examples where Parliament has intervened—in 2010 through the Bribery Act, and in 2017 the Criminal Finances Act. You have to put all that into the basket and then assess whether there are still gaps alongside it. There are one or two areas, particularly in the field of corporate criminal liability, where it would be useful to have a conversation to see if we can go a little further.

Baroness Kingsmill: I was interested because of the complexity; 2006 is a little while ago and crime has changed. I am interested in whether there are more specific offences that might be useful and whether you are able to recruit people who are qualified to deal with those additional offences.

Max Hill: For prosecutors, it is about accumulating experience over time. In what we would have called the Specialist Fraud Division, which is now part of the new SEOCID, we have a concentration of real expertise—in many cases, people who have been prosecuting fraud cases for two or even three decades. The new SEOCID, if I can shorten it to that, gives us an opportunity to pull in some more expertise in certain regions. We rely heavily on external legal advice in the sorts of cases we are talking about, particularly the higher-end, lower-volume cases. We identify specialist counsel to advise pre-charge, so you have a picture of a specialist reviewing lawyer employed by the CPS alongside specialist counsel, Silk or junior, who help to shape the case. That leaves the specialist prosecutor on top of case management, case progression, and disclosure, which is another very significant aspect of work in this area.

We need to grow to improve—back to that eye-watering title of £4 billion to £5 billion per year. In our part of the world, being one of the prosecutors, if I take the last five years, we have secured confiscation orders as a result of our prosecutions in excess of half a billion. We have returned £126 million directly to victims of fraud. That is good, but it shows that there is more that we could do, more of the volume that we need to grapple with together. You need to put our figures alongside what the Serious Fraud Office achieves to get the full picture. I think we should look to do more.

Finally, on resource, we are as good as the legal profession. I hope the CPS is an attractive place to be and to work. I believe it is. Through our panel of external advocates across the Bar, we have a resource to rely on, but we are talking about high volumes of offences and we need

people available with the right skills and interests to do that complex work.

Baroness Kingsmill: Thank you.

Q243 **Baroness Bowles of Berkhamsted:** I will put my question in two parts, but I will give it to you straightaway, up front. The Law Commission has recently reviewed corporate criminal liability and I know the CPS has given input to that. In your view, does the identification principle require reform, and—it is "and" rather than "or"—should the failure to prevent model be expanded to cover fraud? That is the first part of the question.

The second part is about platforms used in the context of fraud. What are the challenges in holding companies to account for fraud that is facilitated by their platforms? If there were a failure to prevent model for fraud, as suggested by the Law Commission, would it extend as far as the platforms? It has said that there should be a requirement to benefit the company, and obviously companies get some revenue from it, but it is a passive thing. Would that be enough to constitute benefit or would they be excluded by such a limitation?

Max Hill: Thank you very much. The answer to part 1 is yes and yes. Yes, we should have another conversation about the identification principle. Yes, I am very interested in broadening the failure to prevent model, because it is not a one-stop introduction; it is already there.

In terms of platforms, whatever we do in answer to the Law Commission report, there will need to be a read-across to other areas of legislation, probably also the Online Safety Bill, for where we are looking and where information and data is being held.

START SUBBING HERE

Can I go back briefly to whether there is a problem with the identification principle? Those who responded, us included, to the Law Commission have come up with a variety of responses; not everyone is calling for the abolition of the identification principle and nor am I, but I am pointing to the practical difficulty. I can go straight to the Barclays plc case in 2018 where the High Court, perfectly understandably, defined the identification principle. In doing so, it defined it on what many would say is quite a narrow footing.

In other words, prosecutors, whether us or the SFO, have to be able to identify the controlling mind of the company, or the identification principle fails and we end up, as in so many cases, effectively prosecuting an individual who was once director of the company. By the time the case has been investigated, you find the corporate model has changed, director roles have changed and you end up with, to put it very bluntly, the responsibility and assets of the individual, when the proceeds of the crime are held within the company, which has managed to move on. That is where a valid conversation should be had.

The SFO has suggested, "Don't abolish the identification principle. Put it on a statutory footing", and I would not quarrel with that. My real interest is in saying to companies, "We all need good corporate behaviour. Everyone should sign up to that". This is nothing new; failure to prevent in a corporate sense is nothing new. Both of the statutes I mentioned earlier, the 2010 Bribery Act and the Criminal Finances Act 2017, have allowed or created criminal offences for companies that fail to prevent. At the moment, they have only done that in bribery and corruption cases, Section 7 of the 2010 Act, and facilitation of tax evasion under the 2017 Act.

It is perfectly legitimate to ask why we do not broaden that across fraudulent activity more generally. To which anyone with a corporate interest would say, "Well, we need to be careful. This isn't a crude mechanism to drag those in the boardroom into the courtroom". There would need to be a defence and that would probably be defined as due diligence, or, to put it another way, "Taking reasonable steps to prevent fraudulent activity in your company".

We have had money laundering legislation for decades across the corporate structure. It is necessary to take reasonable steps to prevent money laundering, and we have the reporting and regulatory regime there as well as prosecution of offences. The same applies here. The great benefit of it is that, in my view, it would drive better corporate behaviour and it would enable the prosecutors to bring a case that drives through to the ill-gotten gains of fraudulent conduct, rather than simply identifying individuals who may have moved out and moved on from the company by the time we get to them.

If you and the committee are interested, clearly a guiding principle would be, "We've got all this money that is going out of ordinary people's pockets. Fraud creates thousands and thousands of victims. We want to do everything we can to put money back in their pockets". We may come on to this: I would like to connect what I am saying about corporate criminal liability and the expansion of that to perhaps a slightly better, more nuanced model of returning the proceeds of crime to victims. Given the opportunity, I would like to talk about the difference between confiscation and compensation, where there is more we can do. Does that answer your questions?

Baroness Bowles of Berkhamsted: It kind of answers the first part. I am trying to get at the difficulty of getting to the platforms that have facilitated the fraud. In analysing the offences that already exist in failure to prevent, the corporate criminal liability options paper, on page 100, paragraph 8.54, says, "We conclude, therefore, that any 'failure to prevent' offences should include a requirement to benefit the company"; that is that the company had benefit from the fraud. It is to exclude where it is a fraud on the company, where they think that the company should not pay a penalty for being defrauded.

By making that provision, where does that leave a platform? We heard evidence in the previous session that, although there is some income

from fraudsters using SIM cards and so on, they reckon they are spending more on trying to prevent those frauds, and the fraud ultimately is on the person who may give away information. With that proviso, would they be excluded from a failure to prevent offence introduced on the Law Commission terms?

Max Hill: I suspect much longer conversations are needed on that. What we are talking about is the extent of due diligence, how far it goes, what reasonable steps are, and what the junction is between that and the way that the corporate entity, to put it very simply, becomes bigger and has a bigger financial footprint as a result of the fraudulent activity. That is why I mentioned the Online Safety Bill, which will be relevant in this context. In criminal justice, the notion of working out the benefit from criminal activity is well worked; that is the confiscation regime.

On conviction, if a corporate, under the model that we are discussing, has been prosecuted and has raised a due diligence defence that has failed, on conviction it will be for the court to determine, as part of the sentencing phase, what the true benefit of the crime has been. That needs to be decided in pounds, shillings and pence so that a confiscation order can be made. Arguments could then be advanced in mitigation as to whether it is a true benefit or not, but by that stage you would know, because due diligence had failed, that you actually have the commission of an offence, and then it is a matter of looking into the company accounts to see how the company has been able to move on, having benefited and done well from the fraudulent activity, as opposed to one that made no gains at all.

In the post-conviction space, that would be very important, but pre-conviction, of course, we would need to allow managers, directors and corporate officers to say, "Actually, everything we've been doing has been preventive rather than committing the offence". That is something the judge and jury would need to work out in the trial phase.

The Chair: Thank you very much. We need to move on. We will later come specifically to a question about victims, and we may be able to go back to the compensation issue then if we have time. I am conscious of your time and of ours, so I am going to move on now to the right Richard this time—Lord Allan—to ask his question.

Q244 **Lord Allan of Hallam:** Thanks very much, Chair. We have heard from the CyberUp campaign, which has been calling for a long time for the Computer Misuse Act 1990 to be amended so that there is a statutory defence for cybersecurity professionals acting in the public interest. In the context of this inquiry, the concern is that cybersecurity professionals may hold back from going after fraudsters because they fear that they may make themselves vulnerable to prosecution by you because they broke the CMA. I am curious to understand your view of the need for a statutory defence and the extent to which you think that cybersecurity professionals' fear that they may expose themselves under the CMA is well founded.

Max Hill: We need to be careful that we do not create through a public interest defence a mechanism that neuters the legislation that is intended to get at offending. The best answer I can give to that question is that at the CPS we always adopt the same tests, and they are enshrined in the Code for Crown Prosecutors. As most people know, there are two elements of the test: evidential sufficiency first and public interest second. In every crime, every prosecutor will need to apply his or her mind to public interest factors. Those factors most obviously are the seriousness of the offence and the level of culpability of the suspect.

The factors, which are in writing in our code, also include whether prosecution is necessary and is a proportionate outcome for the offence in question. Is it a proportionate response? Those who claim to have acted in a particular way out of public interest would have the opportunity to argue that. To put it the other way round, a prosecutor would always consider whether it is proportionate and reasonable to prosecute, as opposed to some other outcome at the end of an investigation. That is the best answer I can give. Again, it is something that merits longer and more detailed conversation.

Public interest is a very well-known feature of prosecutorial decision-making. My advice to those whom you are referencing would be, whatever the law says, to take legal advice and make sure they abide by the law. That is the best safeguard. It is not for me to give options away from prosecution in every case because that would simply neutralise the effect of the legislation. The Computer Misuse Act, which we have had for three decades, is still very useful and very necessary. There is greater complexity and volume in the misuse of cyber spaces and computers, but the essential nuts and bolts of what the 1990 Act says are still used by prosecutors today.

Lord Allan of Hallam: Thanks so much. That chimes with some of the evidence we heard, which was, essentially, that we should rely on prosecutorial discretion for those cases. It would be good as a follow-up if you were able to share any information from your records of instances where people have claimed to be cybersecurity professionals in the way that you described and engaged with the CPS to say, "You shouldn't be prosecuting me". If there are cases like that in your records, it would be interesting to see them.

Max Hill: I do not have any at my fingertips, but I am very happy to write in if we can find examples that would help.

Lord Allan of Hallam: Thank you.

The Chair: We will move off law reform and back on to your home territory, the prosecutorial process. Lord Young has the first question in this space.

Q245 **Lord Young of Cookham:** Good morning. In response to a question from Lord Vaux, you said that part of your role was to highlight real-life examples of difficulties and to help investigators in the performance of

their duties. Turning to the disclosure regime, we heard some evidence from earlier witnesses that it is a barrier to delivering swift justice. What is your assessment of the disclosure regime, and does it require modernisation?

Max Hill: Thank you. I always defer to the Attorney-General's guidelines on disclosure, which is topical because a comprehensive review was conducted by the Solicitor-General, and the Attorney-General republished her December 2020 guidelines only a month ago. It is important to note that, although I have all sorts of specialist discussions about individual crimes or crime types, those disclosure guidelines are fit for all purposes, and we all have to abide by them.

In the field we are talking about this morning, size and complexity create a problem for investigator and prosecutor because what the Attorney-General's guidelines have created is what I sometimes call a front-loading of the system; in other words, do not wait until the case is charged before verifying that there is no material within everything seized by the investigator that might be relevant to the case or, still worse, might undermine it and be relevant to the defence.

Historically, save in some specialist crime types, there has been a tendency to look at the evidence first, get the case charged, and do the disclosure review afterwards. That is what led us, through some celebrated cases, particularly in 2017, into a real problem for criminal justice. The response to that is that you must do this first.

That leads to the necessity in this area under our SEOCID for comprehensive analysis of all the proceeds of an investigation. The example I gave earlier of the case with 28 million files means that they are in the possession of the investigator, and therefore they will all have to be checked for relevance either to build the case or, as sometimes happens, to reveal that the case is not what you thought it would be. There are a number of mechanisms you can use to do that, using computers and setting fields to search for material that could be relevant, but it is still a colossal task, and is shared between investigator and prosecutor.

That takes you to the other big topic in this area, which is GDPR, or redaction. Redaction is a necessity because, a fortiori in this area, where we are discussing fraud, people's individual details and privacy rights need to be protected, otherwise they could be vulnerable. We all know that we have to abide by the data protection regime, and we all know that before we make public use of information it has to be in a suitable form.

There has been discussion, which went on through the review of the Attorney-General's guidelines, about whether you could create a data protection-free corridor, a GDPR-free corridor: "Just let the investigator show the prosecutor everything, and we'll deal with redaction later". The Attorney-General went so far as to say that a proportionality test should be used. If there is a very large volume of material, investigators are

entitled to say, "It is disproportionate to make all of this GDPR-compliant when all we want to do is send it to the prosecutor for discussion and legal advice on the case".

I have to say that immediately following that, when the material comes to us for charging and when we charge—going back to my point about timeliness—we are expected to run through from charge to trial faster and faster. Even though economic crime is probably the slowest area in criminal justice because of the sheer amount of time it takes to investigate, once charged you are really up against it, and you need to provide material in the correct GDPR-compliant format for court. Somehow, we have to create a balance in going through a mass of material.

All of that is not to say that the disclosure regime is deficient. In the Criminal Procedure and Investigations Act 1996, that test, which was looked at by the Justice Select Committee three or four years ago, was not found wanting; it is just that at a practical level we really have our work cut out to make sure that we do everything we need to in good time before proceedings hit a public court.

Lord Young of Cookham: Thank you. That was a very comprehensive reply. We have heard that the data protection regulations place onerous burdens on investigators. Would you go along with that?

Max Hill: I would go along with it, and I would say that in this field 60% of the casework that our new directorate – SEOCID - is looking at is pre-charge advice. The vast majority of it is of high complexity, or even exceptional complexity, top end of the scale, with an investigative strategy that will capture a great amount of data, and that creates a real task for everyone to go through and make sure it is in the right order.

Lord Young of Cookham: Thank you very much.

Q246 **The Chair:** Thank you, Lord Young. Happily, you have taken us to the question I want to ask. I have a very specific question on GDPR about the advice we received from the chair of the Bar. I am sure you have had the opportunity to read the evidence he gave us. If you have not, I would be happy to let you read it and then write to us about this, but I am sure you have read it. He gave us some very specific advice about what he thought could help the situation and help with the barriers or blockages, the bumps in the road that you were experiencing in GDPR. I am going to put some of the things he said to you. I will put them all together and you can then give me a comprehensive answer, as you have been doing so far.

He said that the ICO had fined the CPS. Could you share with us some of the context of those fines? You have told us, which is an answer to the next question I had, that the GDPR has had an impact on the prosecution of fraud cases. He suggested the establishment of a working group between the CPS and the ICO focusing on how GDPR is applied in criminal prosecutions. Do you agree that that would be a good idea? Finally, to

what extent would you seek an exemption for the CPS to allow greater flexibility in that context?

Max Hill: Thank you very much. I will answer in the sequence that you asked. We have been fined twice by the ICO—once in 2015 and once in 2018. That is quite a good record. I am not seeking to airbrush it out, but there were only two fines. One was in relation to video-recorded evidence and the fine was £200,000. That was in 2015. The other, again, was video-recorded evidence. It was lost somewhere along the way to court, and that was a fine of £325,000. We take that seriously, but those are the only two examples. The ICO, like everybody else, has to apply the law. While I completely understand what the chair of the Bar says—a colleague of mine, and a fraud specialist himself—the law is what it is.

On question 2, I think it is always useful to have more conversation, and I have no objection to forming a group, and we would happily be part of it, but that is with a view to ever increasing the understanding of what the ICO is saying to us and, vice versa, that the ICO learns how investigators and prosecutors need to act in relation to the colossal dumps of information that we have to go through, and the law applying to all of it.

That leads to the third question on whether we should have an exemption, which is something the Attorney-General and Solicitor-General specifically considered in refreshing and reviewing the Attorney-General's guidelines. There is no exemption to date and I have not argued for one.

My argument on behalf of the CPS is that we need proper conversation as early as possible, ever earlier. To put flesh on that for a second, I brought out what is known as the Director's Guidance on Charging, volume 6, at the same time as the Attorney-General's disclosure guidelines. That is a way of saying, "We are here. Come to us if you are seeking legal advice".

The next stage is for us to set a strategy for the case, and we have created what are known as disclosure management documents in almost every case now. They go to the judge at the first hearing and they are available to the defence. It is for the defence to say, "These are the issues in the case. These are the aspects we agree with. This is what we don't agree with". I encourage earlier conversation because, on behalf of the prosecuting authority, it helps nobody, and certainly does not help us, when a point on disclosure is aired so late in the proceedings that we do not have the time to deal with it. That is where a working group might be able to have a fruitful discussion.

A GDPR-free corridor strikes me as very difficult. It would be a wholesale opt-out from the law that applied to us all. As I said, the Attorney-General has not suggested that is the way forward. That is where the proportionality test on redaction comes from, and we will work with that.

The Chair: Thank you very much. That is very helpful. I do not need to

follow up, and I do not think any of my follow committee members want to, so I will move on.

Q247 **Lord Sandhurst:** My questions follow from the questions that the Chair has been asking. This is all about the ICO and data protection. It seems to me that you have identified two particular stages. One is material being passed from the investigator to the CPS, and the other is you disclosing material thereafter to the defence.

On the first stage, might there not be scope for some sort of exemption that might speed it up because you are acting together with the investigator, effectively, as part of a team? If they withhold stuff under a flawed view of what might be protected or what is not relevant, that might jeopardise the prosecution, because either it might mean you do not see something that would have been useful and that you could have relied on or, conversely, the whole thing might unravel in court because the defence did not see it.

I am sorry to go on at some length, but this is not just for you; it is for the audience. Is there not a case for having a protocol that at least relaxes things as between the investigators and the CPS, and is that not something you could work through with the ICO and the Attorney-General?

Max Hill: Thank you. An element of relaxation to facilitate the work is something we could discuss, but it would be absolutely essential that, once that conversation has happened and the case is taking shape and looks like it is going to court, the redaction burden still falls—remains where it is—on the investigator. What I cannot have, for resourcing reasons apart from anything else, is a shift in the redaction burden from investigator to prosecutor. We are not resourced for that.

Yes, one could formulate an ideal world in which the prosecutor sees literally everything unredacted at stage 1, and then at stage 2 everything is sent again but in redacted form ready for service in court. The answer is somewhere between the two. To take the simple example of the investigation that generated 28 million files, in complex crime, which is what we are discussing today, we are heavily reliant on expert investigators, who commonly have a dedicated disclosure officer or a disclosure team, with their own protocols and investigation strategy that breaks down the material into what is genuinely relevant to the offences in mind. If we do not have that and we create a statute-free corridor, there is a risk that the prosecutor would simply be told, "This is the product of the investigation. Please go through it". That is putting it more crudely, of course, than you suggest, but there is a real need at the very earliest stages to set the right strategy, which in turn will dictate how much material is seized and what thought is given to why it may be relevant.

Instead of a statute-free corridor, we actually need—and this is fuelled by my guidance on charging—an earlier conversation between lead investigator and potential prosecutor at which the investigator will say, "This is what we've got. This is the strategy we have set", and that can

stem the flow of the material, and the size and shape of the material, if you get it right. If you get it wrong, you can end up not seizing material that is highly relevant. If you do not do it at all, you can end up seizing far too much and having a warehouse, almost literally, of information that it is impossible to work through, whether you have strict application of GDPR or not. There is no substitute, in my view, for early conversations breaking down the nature of the task so that it remains manageable.

GDPR and DPA compliance must remain where it is at the moment, with the police or other investigators, so that at the final stage we are presented with a clean file that we can put into good order to present to court. Once we fire the starting gun on a prosecution, as I need hardly tell highly qualified lawyers, the clock is running, and we need to act with great speed.

Lord Sandhurst: Do the investigators need more resources?

Max Hill: We need to be appropriately resourced. Undoubtedly that is right. I can only speak for the Crown Prosecution Service. The headlines, I am afraid, are well worn. Since 2010, there has been a reduction of 44% in budget and 30% in headcount. It is only the spending review of 2021 that has given us an influx on a three-year basis, which was crucial, to allow us to build through 2022 to 2025. I am grateful for that. I am not sitting here saying that we are inadequately resourced, but we need what we have, and we have to grow the organisation in order to improve and in order to do what we are all interested in, which is to grip more of the national loss to the country through fraud that is happening year on year.

Lord Sandhurst: Is there one thing that, if the ICO was agreeable, you would like it to do?

Max Hill: We have a very constructive relationship with the ICO. There is a great deal of mutual respect on either side. It is about pausing to understand the complexity and the difficulties before rushing to judgment. I do not want that to sound critical because that is what the ICO does. We have a series of statutory schemes that apply at all stages, and they impact on many components of the system. Perhaps, dare I say it, the fact that the two fines I pointed to are now of some age shows that we have educated ourselves and each other into the nuances of the system. I do not have a shopping list for the ICO beyond continuing to understand how difficult it is for front-line prosecutors, particularly in this area, to deal with such high volumes of information and material.

Lord Sandhurst: Thank you very much.

The Chair: Can I ask a question that may be deceptively short? It allows a relatively short answer. Is there a case for specialist courts for fraud cases and, if so, what would they look like?

Max Hill: Yes, we welcome the City of London courts and the economic crime focus in the new City of London court that is coming, I think, by

2026, which is the date I have heard. It is helpful to be able to take specialist cases to a dedicated court. In fact, the Nightingale spaces across London, some of which are still operating, were useful to this division of the CPS, and we were able to encourage the judiciary to place some of our cases before the courts even as we went through the pandemic.

That said, I completely recognise that there is a national case load backlog, which we have all been working terribly hard to try to bear down on, and it can be very difficult to prioritise one area of important crime over another. In the last week, we have heard a suggestion for specialist courts to deal with adult rape cases. I am discussing an element of specialism in courts to deal with economic crime. As the chief prosecutor, I encourage all of that because I see the priority behind the work and the urge for justice, in some of these cases, for hundreds, if not thousands, of victims of fraud. We want to do that as soon as we can.

The Chair: Thank you very much. There is after all, we are told, in excess of 40% of personal crime in this country.

Q248 **Lord Vaux of Harrowden:** We have heard about the barriers that prevent effective prosecution of court cases, such as court capacity, and you have talked about the complexity and time and so on of criminal prosecutions. Is there, in your view, an argument for greater use of civil remedies or regulatory sanctions to tackle the issue?

Max Hill: The short answer is yes, but not as a substitution for criminal process. Clearly, for my organisation, the clue is in the name, as they sometimes say. We are prosecutors, and we are here to take cases to court, to do it in public and to deliver justice for the public and in public.

In that context, may I say that I remain absolutely confident in the jury system and in the ability of, as it were, ordinary people to decide on complex fraud? It is our job as prosecutors to make it comprehensible and to present it in a clear fashion. There is enormous value in delivering justice publicly through criminal process. You cannot say, "Let's just move to civil process because it's easier or quicker". You have to maintain the public function. That said, there are some statutory civil powers that are available technically to me, which I can delegate to other prosecutors, and we are using them.

Following the lead of the National Crime Agency, in very recent years we have been looking at civil models and at civil asset freezing and forfeiture, and we have had some early successes with that. I am keen to maintain that, but I would not want to give an impression that, because fraud is about money, we will simply go for recovery of the money without identifying and prosecuting the perpetrators of the fraud, which must remain our primary focus.

Lord Vaux of Harrowden: It would be interesting to receive afterwards examples of the sort of thing you have just mentioned, the civil remedies you are using.

Max Hill: I am very happy to do that. In the letter that is coming, I will add a section to tell you about early civil forfeiture cases, because we have had some significant cases in the last year to 18 months.

Lord Vaux of Harrowden: That would be helpful. The key thing, ultimately, while it is great to get these people banged up and into prison or whatever, is to try to reduce the levels of fraud and the numbers of victims. It is such a huge problem at the moment.

On the regulatory side, do you have ideas about how we can push that forward with the aim of trying to reduce the numbers? I understand that your role is to prosecute the criminals, but we have to do something to reduce the numbers.

Max Hill: Clearly, I am not the expert on the regulatory front. I referred earlier to the regulatory scheme in relation to money laundering and the reporting regime there, which has been effective. It brings about a sense of better corporate behaviour as well as providing a mechanism for bringing activity to the attention of investigators, but, again, that sits alongside the criminal process powers under Proceeds of Crime Act legislation. You need both. My suggestion in relation to corporate criminal liability is that you can only get so far through regulation to really bear down on bad corporate behaviour, which, of course, is a very small minority, but it is still something we need to worry about. In order to bear down, you need the force of criminal process as an available tool alongside regulatory mechanisms.

It might be a very difficult argument if we had no corporate criminal liability on the statute book, but I have given two examples where we do, and I have yet to hear a good argument as to why that should not be expanded across broader areas of fraud and economic crime more generally, subject to a defence such as taking reasonable steps due diligence. I am not talking about creating offences of strict liability—there are very few of those on the statute book wherever you look—but we need the tools available, because to get to the money and then to get that money back to those who have lost it means that we need a hybrid between regulatory encouragement and prosecution enforcement.

Lord Vaux of Harrowden: Which takes us back, I suppose, to some of the discussion about the failure to prevent that we had previously. In that discussion, I am not sure whether we quite got to the difference between the company being directly responsible for the fraud and benefiting from it versus simply the company's services being used by the fraudster and the company taking measures to prevent the fraudsters using their services. How do we attack that? [*Inaudible.*]

Max Hill: Obviously, there is a key distinction between the two. That is why, understandably, in the Barclays case the High Court gave a strong but quite narrow definition in applying the identification principle. You need to identify the controlling mind of the company, and, if you cannot, that principle fails. If we were to extend corporate criminal liability, we would need to do it for the right reasons, not to go after companies that

have a bad actor in their midst who is abusing their processes, but to go after companies that know about that or have looked and not taken sufficient and reasonable steps to guard against it.

In the same way that we are now using Section 330 of the Proceeds of Crime Act, which is to do with a prosecution, albeit against an individual who suspects money laundering activity even where none may actually be proven, we need a corporate concomitant to that to say, "This is, or may be, going on under your roof. You are safe from prosecution if you are exercising due diligence. If not, we have a model that can bring you into court". We need that. If I may, I will link that, unless stopped, to what we are trying to do, which is to get the money back to those who have lost it.

To expand that for a moment, on conviction, a court assesses the benefits of the crime, makes a confiscation order, and people are often mystified by a benefit figure—to take a simple sum—of £10 million but a confiscation order of £1 million. That is because the realisable assets at the time of sentence are only identified at £1 million, but the reason you set the benefit high is that later revelations—later investigation—might reveal £2 million to £5 million. You then go back to court, amend the confiscation order and take more of the proceeds of the crime.

That is in contrast to the compensation regime—it is only a compensation order—that puts money back into the pocket of the individual who has lost it, the victim of fraud. That compensation regime is effective and can be imposed at the time of sentence, but there is no power to revise it. If the realisable assets are low, compensation can be impacted by that. Even if further assets come to light, you cannot go back and say to the court, "Could you upwardly revise the compensation order? We are now in a position to get more money back to victims".

That should be looked at. It is a statutory change that could be made under the court sentencing provisions, and it would be very beneficial. I can only emphasise that, using the powers we have, we do everything we can to return money to those who originally lost it, and we should look to increase that over time.

The Chair: Thank you. We continue on that theme because we are going to turn to the most important people in this whole terrible environment—the victims.

Q249 **Baroness Kingsmill:** I have a comment on what you said before, Mr Hill. I must say that something like the Bribery Act has been extremely effective in affecting corporate behaviour. Whatever the number of prosecutions that have arisen from it, it has nevertheless had a huge impact on corporate behaviour in practical terms in the way they educate their members of staff and other people about how to recognise and avoid fraud. It has affected their behaviour significantly, so something similar is probably what we need.

To turn to the victims, to what extent does the CPS feel that the victims

are its responsibility? To what extent are they supported during prosecutions? What arrangements are in place to enable them to get compensation? You very kindly distinguished confiscation and compensation. The victims are probably more interested in the latter.

Max Hill: Compensation is a system that works on the basis that the investigating team will give a very clear account of the loss to the victim, provided that is escalated to the court in time. On the point of conviction, a judge has the power to order compensation, and always will if that is possible. My point is simply that it is a one-stop chance to calculate compensation. I think there should be two stops, as in the confiscation regime where you come back and revise it upwards if the money becomes available.

Baroness Kingsmill: It is always a case of deep pockets, is it not? If the perpetrator is a telecoms company or a bank and has not done sufficient to prevent the fraud taking place, they have deep pockets, and they are the people from whom you could extract pretty significant compensation on behalf of victims.

Max Hill: Yes. That is a further point in favour of an extension of corporate criminal liability. QED, a fraud is as large as the amount of money taken from the victims of that fraud. That money has always gone somewhere. It does not disappear. It may be carefully hidden. It could be within a corporate structure or it could be onshore or offshore through whatever mechanisms an individual perpetrator has used to hide it. We need to do everything we can to uncover that sum. Those with very deep pockets at the time of conviction are easy to deal with. Those who have managed to hide the funds from their ill-gotten gains for use later should not feel that, because they have got through the sentencing hearing, they are safe from further scrutiny. That was my point.

There is a very strong shared responsibility right across the criminal justice system to inform and look after victims. It does not exclusively fall on the CPS. It is shared between the police and third sector services, often locally commissioned, in police force areas. It is undoubtedly shared by us. There is a role for the Courts Service through the witness service scheme, which is excellent, up and down the country.

It has been only too well publicised that a lot of research has shown, particularly in the field of sexual offending, that we, the CPS, are not doing enough to give information at the right time to those who need it, and that is why we have commissioned comprehensive research. We call it a victim needs assessment. We are only too well aware of the Victims Bill and the consultation around that. We are now formulating what will be a properly enhanced offer for victims of, in particular, adult rape, but I do not want to stop there; I want us to look at the aspects of crime where there is, if I can use the phrase, higher harm, so that where historically we have created an enhanced offer to bereaved families in homicide cases, which sits within quite specialist casework, we need to do that for higher harm cases across the piece. That is where it has to be a differential offer.

The CPS is not resourced to take over all witness handling in the hundreds of thousands of cases that we bring each year. The policing organisations are far larger than us. We need to continue to rely on all the great work they do through witness care units, but we need to do better in specialist areas in giving information to the victims of crime who want it. Not all do, but those who do must have a better service from us, and it should not be restricted to the occasional letter; it should be through actual conversations face to face. That is what we are formulating.

Where we can, that will be a feature in this area, although in investment fraud, which creates hundreds or even thousands of victims, I hope everyone can understand that the operating model would very quickly collapse if there was a one-size-fits-all mandated scheme of contact between prosecutors and victims. We have to be sensible about it. The bottom line is that we have not been doing well enough in communicating with victims, and we have to do better.

Baroness Kingsmill: Thank you.

The Chair: Thank you very much indeed. Happily, we have come to the end of this session on time. First of all, Director, thank you very much for your time this morning and for the obvious time that you have put into the preparation that you must have done to come and give evidence to us. I will put it this way: the crispness and relevance of your answers have been of great help to us. I do not think we are surprised by that. You certainly have not disappointed us. You have given us a lot of good evidence that we can work with.

On one or two occasions, there was discussion of possible follow-up. We will take responsibility for that and write to you to remind you of the few points that you said you would engage further with us on. Thank you very much indeed. I now formally end the meeting. Thank you very much.