HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: Government use of data analytics, HC 891

Thursday 15 January 2026

Ordered by the House of Commons to be published on 15 January 2026.

Watch the meeting

Members present: Sir Geoffrey Clifton-Brown (Chair); Mr Clive Betts; Sarah Green; Rupert Lowe; Catherine McKinnell; Blake Stephenson.

Gareth Davies, Comptroller and Auditor General, National Audit Office; Joshua Reddaway, Director, National Audit Office; and Edward Pinney, Alternate Treasury Officer of Accounts, HM Treasury, were in attendance.

Questions 1-97

Witnesses

I: Mark Cheeseman, Chief Executive, Public Sector Fraud Authority; Emran Mian, Permanent Secretary, Department for Science, Innovation and Technology; and Conrad Smewing, Director General, Public Spending and Joint-Head of the Government Finance Function, HM Treasury.

Examination of witnesses

Witnesses: Mark Cheeseman, Chief Executive, Public Sector Fraud Authority; Emran Mian, Permanent Secretary, Department for Science, Innovation and Technology; and Conrad Smewing, Director General, Public Spending and Joint-Head of the Government Finance Function, HM Treasury.

Q1 **Chair:** Welcome to the Public Accounts Committee on Thursday 15 January 2026. The NAO estimated that fraud and error cost the taxpayer between £55 billion and £81 billion in 2023-24. Data analytics are a vital tool to help tackle fraud and error, ranging from payment checks to the use of emerging technologies, including AI, to help Departments identify risky transactions.

The Government Digital Service, which we will refer to as GDS—the digital centre of Government—believes that data analytics could prevent up to £6 billion in losses from fraud and error. However, despite their considerable potential and central availability of useful tools, data analytics are not being used widely enough by central Government Departments. It has also recently been confirmed that the role of chief digital officer at DSIT has been scrapped.

Today's session will be an opportunity to examine progress made in promoting the use of data analytics to tackle fraud and error across Government, as well as to challenge Government on their plans and explore barriers to implementing data analytics on fraud and error more widely. We will also be exploring how Government are striking the right balance between the level of transparency in their use of data analytics with the risk of making it easier for fraudsters to take advantage. Today, I extend a warm welcome to Emran Mian, who is the Permanent Secretary at DSIT—thank you for coming. Would you like to introduce yourself and, as its your first time, just very briefly say a little about your background? That would be very helpful.

Emran Mian: Thank you, Chair, and good morning, everyone. My name is Emran Mian, and I became Permanent Secretary of the Department for Science, Innovation and Technology in July last year. I had spent two years prior to that in the Department as the director general for digital technologies. Before that, I held roles in the Ministry of Housing, Communities and Local Government, the Department for Education and a couple different versions of the Business Department. I have been a civil servant since 2002.

Q2 **Chair:** Thank you for that. We now have two very senior civil servants either side of you. Conrad, you are from the Treasury. Do you just want to introduce yourself briefly? You are a regular at the Committee, for which we thank you.

Conrad Smewing: It is nice to be back—happy new year. I am Conrad Smewing, and I am director general for public spending and co-head of the Government Finance Function.

Q3 **Chair:** Thank you. Mark, you are also a regular at the Committee, so thank you. Could you also introduce yourself?

Mark Cheeseman: I am Mark Cheeseman, the chief executive of the Public Sector Fraud Authority and the head of the Government Counter Fraud Function.

Chair: Thank you very much. To start us off today, we have my very able deputy, Clive Betts.

Q4 **Mr Betts:** The public always have concerns about how much the Government spend, but they get even more concerned if the money is not spent properly. Fraud and error is a big issue, and I think people watching this hearing today will probably be astounded at two things. One is the estimate that the amount of fraud and error could be between £55 billion and £81 billion, so the sums of money are potentially very large. Secondly, there is the lack of clarity and accuracy about what the figures could be—£55 billion to £81 billion is a very wide range, isn't it? In other words, nobody really knows, do they? What are you doing to make sure that you can have a better grip of what fraud and error actually amounts to?

Mark Cheeseman: The numbers that you have used are absolutely right: £55 billion to £81 billion, which is fraud and error across central Government. It is a large figure—there is no denying that—and £40 billion of it is tax, £10 billion is welfare and the remainder is the rest of the system. Also, it is the level—it is not necessarily the loss, but the level—of fraud and error in the system. I think that is an important point to dwell on. The methodology adopted does not take into account all the things that Government Departments and public bodies do to reduce it. You heard from the DWP before Christmas talk about the work it is doing to reduce fraud and error in the welfare system, as well as the work that is going on to reduce fraud in tax gap. It is a gross figure, not a net figure.

You are absolutely right that it is a big figure, but I would point to the fact that we are one of only three countries or blocs—that I know of—that have an estimate of the overall level. The first is us, the second is the United States and the third is the European Union, and when you compare our level with their levels, actually they are broadly similar. In the United States, in the recently published 2024 GAO report, it had a range, and its range was 3% to 7%. Our numbers work at 2.8% to 4.1% of expenditure and income. The European Union published the midpoint of its range, and its number is 3.6%. Again, they are comparable with the numbers that we see in the United Kingdom.

I also look to other sectors. There is something called the Association of Certified Fraud Examiners, which produces a report every year from people in all different countries around the world. Its estimate of the losses due to fraud that would be expected is around 5%, so the number is big. I completely note that it is big, and that is why the Public Sector Fraud Authority exists. That is why investments are being made to do more and to reduce that number and to have a bigger impact, but the

number is also comparable with those few other comparators that we can see elsewhere.

Q5 **Mr Betts:** I am not sure how reassuring it is for the taxpayer to know that we are as bad as everyone else. That is basically what has been said to us. What is the plan to get the figure down to a smaller one within a given timeframe? We know, as you said, that DWP has been to the Committee, and it has given estimates—whether we accept them as reasonable ones at this stage—of its attempts to reduce the amount of fraud and error in the foreseeable future. What is being done for the rest of the organisations apart from HMRC and DWP? Is there a plan there? Is there a target that the Committee can know about?

Mark Cheeseman: If this is okay, I will touch on HMRC and DWP first because, of the £55 billion to £81 billion, they are £50 billion. It is a big chunk, and quite rightly, that is where the Government are investing the most. The Government have invested over £700 million into DWP and HMRC, and that is resulting in, or is expected to result in, billions of pounds of reductions.

Your challenge, quite rightly, is the rest as well. The range, which is a range, is there. Since the Public Sector Fraud Authority was introduced, we have agreed targets with individual Departments. In the 2023 Committee, one of your challenges to me and the others sitting here was that only 8% of public bodies had financial targets for what they were doing on fraud like those that DWP and HMRC have. Now all Government Departments have targets, and we agree those targets with them. Those targets are leading to an increase in the impact they are having. In the last measured year, which was 2023-24—we are currently still assuring last financial year—there was a 65% increase in the impact it was having through preventing and recovering fraud.

That is part of the plan that you asked about. The first part is to have a framework where targets are agreed and agreed with the centre of Government. The second part is that Departments are investing more to get to those targets. We can see that in the figures we collect and what the investments are going into. We are going to talk about data and analytics today: the investments going into data and analytics have increased, as have the number of people working in those spaces and the number of people working in other spaces.

Part of the plan is to deal with fraud. The inherent nature of fraud and related error is that it is a hidden crime. Fraudsters are good at hiding what they do, when they are good fraudsters. Part of our purpose is both to understand and to have a bigger impact. Part of the approach to get at that number more quickly is what we have done on fraud risk assessment across Government. All public bodies have fraud risk assessments. They help them to understand where to look and how to have a bigger impact, and as I have noted, the impact that public bodies are having is growing.

Q6 **Mr Betts:** Okay, so everyone wants to work together to get fraud down. That is the general understanding. Everyone has targets. You are saying

that all public bodies and all Government Departments have targets.

Mark Cheeseman: Not all public bodies—sorry; there is a differentiation there.

Q7 **Mr Betts:** Which public bodies do not have targets then?

Mark Cheeseman: I happily come back to the Committee on that. We agree the targets with the main Departments to start off with, and then that filters down through arm's length bodies. There are a lot of arm's length bodies.

Q8 **Mr Betts:** Are those targets public?

Mark Cheeseman: They are not public at the moment, no.

Q9 **Mr Betts:** Why?

Mark Cheeseman: Because they are an internal agreed target between the centre and Departments.

Q10 **Mr Betts:** DWP makes public its targets—that is a big Department with a big challenge. Why can't we know about other Departments'?

Mark Cheeseman: I would say that target setting for the others is quite a new area. DWP has set targets for a long time—you have had the debate with it as a Committee for quite a long time, so that is a more established thing. But this is also a fair challenge, yes.

Q11 **Mr Betts:** Yes, I think it is. Because targets are new does not mean to say they are any less relevant, does it? The fraud is still there, whether it is a new target or an old target.

Mark Cheeseman: The current policy is that we agree targets between the centre and the Departments. Among all the other targets, they are agreeing on lots of different areas as well—they have lots of different key performance indicators that they are agreeing with the centre of Government.

Q12 **Mr Betts:** I think this might be something that Committee members will want to push back on: why can't the public know what the challenges that the Government and Departments have set for themselves? In the end, all those targets individually must add up to a total target, mustn't they?

Mark Cheeseman: Yes, and we report on the total target and the total impact of all those bits in our reports.

Q13 **Mr Betts:** By the end of this Parliament, what is your target to get the figure down?

Mark Cheeseman: The target for us as the Public Sector Fraud Authority or the target across Government?

Mr Betts: Across Government.

Mark Cheeseman: We set targets on an annual basis at the moment, so we do not have one for the end of this Parliament. We have targets for the end of this year, which is to reach—

Q14 **Mr Betts:** And next year? Is it one year at a time?

Mark Cheeseman: One year at a time. The reason for that is because resources are set on an annual basis. As the resources and plans are being agreed, we agree the target. Part of the method of our agreeing a target is that we look every year for an increase in what Departments are achieving in acting on fraud and error. It is an annual process at the moment.

Q15 **Mr Betts:** Some of these efforts to reduce fraud and error are long term—they are about changing the way that Departments do things and giving them more information, but we will come on to some of those in due course. But surely you cannot do this on an annual basis and say, "Right, we are doing this until the end of March, and then we're going to start again in April."

Mark Cheeseman: Having annual targets is a significant shift from where we were before, since the last Public Accounts Committee. I agree there are different ways that one could do targets, of which currently we do annual targets.

Q16 **Mr Betts:** Because it is better than it was doesn't mean to say it is as good as it should be, does it?

Mark Cheeseman: That is a fair challenge.

Mr Betts: Okay. I think we might take on that challenge.

Q17 **Chair:** Conrad, are these targets fully costed by each Department? Has the Treasury given them an allocation? I hear on the grapevine that at least one Department is trying to resile from using its allocation for this digital work to use it for other purposes. What discipline is the Treasury instilling on Departments to ensure that they use this money for digital, particularly fraud prevention?

Conrad Smewing: As Mark was saying, the big money, both in terms of the fraud and the investment that we are talking about here, is in DWP and HMRC. There we have quite a well-established process working with those Departments, where together we assess what the likely returns are on further investments, what kind of investments they can make to get social security benefit fraud and error down and increase the tax gap. That gets built into the OBR forecast each time. Those measures are costed, and the OBR makes an assessment of how effective they expect them to be based on how effective they have been in the past. That process works relatively well. For those big elements of fraud, the OBR has a forecast of the tax gap falling by about 0.7 percentage points by the end of the forecast. DWP came to this Committee before Christmas with its expectations.

For the smaller areas where we are making investments—a lot of those are digital investments—the process we have gone through is essentially

allocating money from the transformation fund in the spending review, which has gone out to Departments to modernise their infrastructure and allow them to use more data analytics to address fraud. We keep track of those investments. I do not know which Department you are referring to that is resiling from that investment, so I cannot comment on that specifically.

Q18 **Chair:** I think they came to the Treasury to ask if they may use this money for other purposes. The thrust of my question is that, if that is correct—I am not asking you to confirm or deny it—is the Treasury using its disciplinary measures to make sure that they do not do that?

Conrad Smewing: I do not know the case that you are talking about. In general, we do not ringfence all departmental expenditure. There is a balance to be struck between allowing Departments to prioritise their funding on what they think should be the most important thing for them to do at the start and having very tight central control of this sort of expenditure. In most cases, outside of HMRC and DWP, the incentives are quite well-aligned for Departments; the fraud is coming out of their budgets, so expenditure to tackle that fraud saves them money. I am not sure there is a case for us to ringfence in general at every stage of those investments, but it is certainly something that we would look at carefully. Not necessarily in counter-fraud but in digital investment more generally, which is intended to improve the productivity of public services over the long run, the Treasury has a strong interest in ensuring that that is not taken away and used for more day-to-day pressures.

Chair: I may come back to that theme. We all know that DWP and HMRC are the good guys—well, the relatively good guys—because they have so much to gain. On the other hand, they have so much more that they could gain, being such large Departments, so I am concerned. It appeared that Mark's answer to Clive was, "We are not really working on the Next Steps agencies yet." There is an awful long way to go on this subject. It is the laggards who are not even beginning on this process or are very slow that I am concerned about. But I will come back to that.

Q19 **Catherine McKinnell:** I want to follow up on the conversation about targets. If I am not mistaken, I think you were going to say what the current target is. Are you able to share with us what the current target across Government is?

Mark Cheeseman: The current cross-Government target for non-HMRC-DWP is around £450 million of impact prevented and recovered.

Q20 **Catherine McKinnell:** Okay. That does seem small compared to other parts of Government.

Mark Cheeseman: If we go back to the estimates, for the £55 billion to £81 billion, £50 billion of that is HMRC and DWP—£2 billion or £3 billion upwards is the estimate there. I agree that there is less maturity in those Departments, so they do not have the infrastructures that HMRC and DWP do. Certainly, the approach of Government at the moment is that every year we are working with Departments to increase that impact and do

more. But as the Report points out, there are challenges to taking action on fraud and error as well.

Q21 **Catherine McKinnell:** That is what I was going to ask. By setting annual targets and not publishing them, is there a risk that it leaves it open for you to revise those targets up—but also down—and has that been factored in? Why are the targets not published?

Mark Cheeseman: Because the current decision is to work with Departments to explore that. I can assure you that they are not revised up or down—that is what we are there for. We set the targets with Departments. It is explicit in our mandate that the Public Sector Fraud Authority sets the targets with Departments. Also explicit in our mandate is that we then share that with the National Audit Office, so the NAO would see if we were starting to move targets up and down with Departments. The system holds the system to account on that.

Q22 **Catherine McKinnell:** I meant on an annual basis. Given that at the moment it is only set out on an annual basis, and since there is no public vision on whether those targets are being met or not, the following year's target could be revised down rather than up. Is that the thinking behind it—to leave scope?

Mark Cheeseman: No. The intention is to increase levels every year. Obviously, that is an individual discussion with each Department, based on all the factors and threats that they are facing. The collective number increases each year, and that is the intention as well. No, the reason is not so that it can be varied up and down.

Q23 **Catherine McKinnell:** The challenge could be that it is under ambitious, rather than over ambitious.

Mark Cheeseman: I understand your point, but I would reflect back that it is significantly ahead of, and a significant improvement on, the numbers we had previously.

Q24 **Chair:** Catherine, I am sorry to interrupt, but will you permit me? Gareth, when you are auditing the accounts of all these Departments, will you be auditing against these targets?

Gareth Davies: The targets are not disclosed in the accounts themselves, although, of course, the level of fraud and error is separated out, particularly in the case of the two main Departments we have focused on. We report to this Committee every year on significant errors of fraud, as you see each cycle. As Mark says, we have visibility of performance against the targets for each Department, so if there is anything significant that the Committee needs to know about, it will come through that process.

Q25 **Chair:** Would it not be much more effective if they were published? We could then see in the annual report and accounts whether they have achieved those targets or not.

Gareth Davies: Transparency is a good thing. In the area of fraud, the issue is not so much whether it is embarrassing to the Government as whether it is giving information to fraudsters about where the investment is being focused and where counter-fraud activity is being targeted. That is the balance to strike, but obviously transparency is generally the right thing.

Joshua Reddaway: The other thing to recognise is that we are talking here about targets for how much the counter-fraud teams will prevent and/or recover, and it is mainly focused on the counter-fraud activities, whereas when you talk about the overall level, a lot of that—if you think of the counter-fraud as a tier 2, they are separate to the frontline. The estimates are actually on what the frontline service is doing.

The area where we have been focusing regarding transparency in the accounts is where there are significant issues in significant areas of expenditure. Our belief is—and the Treasury has now put this into the PES guidance for all central Government Departments—that that should be disclosed in the performance report. We are seeing a general improvement in the level of transparency of that. You are starting to see smaller versions of that £55 billion to £81 billion estimate for each Department in specific areas. Our hope is that if you get visibility of where you have transparency there, you will start to see those numbers come down. But I would say it is still the exception rather than the rule that these things are disclosed.

Chair: That is really helpful. We will want to consider all that evidence in our report. Catherine, I am sorry for interrupting you.

Q26 **Catherine McKinnell:** That's okay; that is really helpful. Thank you.

I want to ask specifically about the £6 billion figure that the Government Digital Service is hoping—perhaps believing—can be saved by using data analytics to tackle some of the fraud and waste that we see. The figure itself does not appear to have been derived from very wide data examples, so I just wanted to get your reassurance that you are still confident that £6 billion is a realistic expectation.

Emran Mian: The £6 billion target was not intended as a target to measure performance against. What we were trying to do in the review of the state of digital government was to provide an illustration of what benefits could be possible across the public sector if we improve data and digital performance. We did that by looking at the service improvements for users that we could drive, as well as the savings for the system that we could drive. The target was one of the illustrations of where we thought there could be benefits. When we get tighter on the analysis of the benefits, they will be a combination of strengthening the data assets themselves and then applying data analytics to them.

One of the challenges we have at the moment is that a lot of the data that you would rely on to then do analytics is not in a good enough state to be able to do data analytics, either because it exists on legacy systems or

because it is not at the right level of data quality. Part of what we were trying to illustrate was that those investments are needed.

When we published the review of the state of digital government, we obviously also had a mind to the spending review process and looking to make the case for why these investments should be prioritised alongside other investments. We were successful in that: the spending review was a very good spending review from the point of view of investing in data and digital across Government. Obviously, Departments are engaged in the detailed business planning now for the financial years ahead. But at an aggregate level, it looks something like a doubling of data and digital spend compared with the previous spending review. I think we have been successful in making the case that there are benefits to be gained here, even though the benefits that we gave in the report were illustrative rather than precise.

Q27 **Catherine McKinnell:** That is helpful, because there is a concern that it does not seem to have been derived in a particularly sophisticated way, but as you say, it is to make the case for broader investment in these facilities. That then begs the question: what is the plan now for improving the use of data analytics to combat fraud and error? You have made the broad case; what is happening in detail to achieve this?

Emran Mian: I can run through the elements of the plan. The first part is that we need to get much better at identifying the key data assets that exist across Government for all kinds of purposes, including these purposes. We have been doing that work with Departments to get a much better register of what the data assets are. One of the criteria we have been using to identify which data assets to think about is exactly which data will be useful for the detection of fraud and error. That is step one.

Step two, which we are doing with a selection of those datasets at the moment, is to get clearer on the characteristics of those data assets—what is often called the metadata—so that we can then begin to assess their data quality. We need to sort improvement plans for those data assets to get them up to the standard where they can be used to run analytics off, and have common standards across them. Again, if we do not have common standards across them, we will not be able to run common data analytics across them. That is step two.

Step three is creating a single exchange or a platform, where, if you want to be able to use one of these data assets, you can discover what data assets are available, and you can, through a single platform or single exchange, be able to start to use those assets. We have built that platform, and it is in a beta test at the moment with a small number of users. That is step three, if you like.

Alongside all that, recognising that we should not be waiting for all of this to be completed before more data sharing takes place, we have also been running a data-sharing network of experts, which has been helping Departments where there are specific challenges to do with data sharing. Those might be practical challenges, such as the data quality, challenges

around policy and standards, or challenges about the interpretation of the law and whether it is possible to share the data in a way that is legal, responsible and ethical. We have an experts group that is helping to broker solutions to those things with Departments.

Q28 **Catherine McKinnell:** What is the timeframe for seeing some of the results? What has been projected?

Emran Mian: We will be setting out an overall road map on the improvements we are seeking to make to data and digital across Government. We had hoped to do that before Christmas—indeed, I think both officials and Ministers said to Parliament that we hoped to do so before Christmas. We were not able to, but we are hoping to do so very imminently, this month. That road map will cover the full spectrum of improvements that we are looking to make in data and digital, and will say more about some of the improvements I have just talked about, which improve the overall data infrastructure. That will put us in a much better position to be able to run data analytics on top of, to be able to tackle fraud and error. That is the next part of the plan.

Q29 **Catherine McKinnell:** In overseeing this from the Department for Science, Innovation and Technology, do you feel you have the means and the levers to get the maximum impact across Government Departments?

Emran Mian: I think we do. The things that give me confidence about that are the combination of the work that we were able to do across Government to illustrate the challenges ahead and the benefits that we could get, in the state of digital government review. We have also now been able to work with all individual Departments to set out what they are doing on data and digital, and to be able to bring that together. That is the publication we are hoping to do later this month.

The other thing that gives me confidence that this is working well is the successful spending review outcome, where we were able to work with Government Departments to prioritise spend on data and digital against other things that they may be doing, in what was a very tight fiscal environment and a tight spending review. The overall spend on data and digital, as I was saying a couple of minutes ago, has gone up very significantly based on the previous spending review.

Those are some signs of the success that we are having so far, but we do not underestimate the challenge of making this transformation in practice. The next three years—the three years of the spending review that we now have funding for—are going to involve a massive team effort across my Department, through the Government Digital Service and the digital functions in Departments.

Q30 **Catherine McKinnell:** Will the road map, which you said is to be published shortly, have clear accountabilities within it and clear timelines and timeframes for when we are going to see the changes coming to fruition?

Emran Mian: Yes, that is exactly what we have been trying to do: set out the things that the Government Digital Service itself is delivering. There are some programmes to improve data and digital across Government, on which GDS itself must be accountable for making sure that they happen—for example, setting up that single data exchange or platform, the One Login programme and the improvements in the gov.uk domain. There is a whole set of things where GDS is itself accountable, and we will be setting out what those are and the associated timescales.

Lots of the improvements here are for individual Departments to lead on. An example is all the work on the NHS app, which has had a very successful opening. It had a lot of improvement and development for that. The DHSC is responsible for those and, again, under the road map on digital government we will set out what they plan to do and their accountabilities.

Q31 **Catherine McKinnell:** Are there sufficient incentives within Government Departments to make the investments needed to then see the results? I mean that in the sense of, rather than those savings being seen across whole-of-Government budgets, Departments themselves being able to see the results and outcomes from the investments they are making, and then reap the rewards of those savings in terms of their ability to reprioritise that funding within their Department priorities.

Emran Mian: A lot of the time, the incentives are really well aligned. If you are able to use the NHS app to provide patients with a much cleaner, quicker, simpler approach to booking appointments, that delivers lots of wider benefits for the healthcare system as well. That is an example where incentives are very well aligned.

Catherine McKinnell: That does not really touch on error and fraud, though.

Emran Mian: No. I was going to say that that is sometimes where the incentives may not necessarily be aligned. You might have a Department that is the data holder, and they are the ones who would have to invest in making the data quality higher, and in providing the data to somebody else, but the other Department would get the benefits from that. That is the classic space where we, as the Government Digital Service in DSIT, need to operate, which is why we are prioritising, within the work we are doing, the creation of, for example, the single exchange or platform, to make data sharing as simple as possible.

Q32 **Catherine McKinnell:** To make sure that I have covered the full panel, what do you need from the Public Sector Fraud Authority or, indeed, the Treasury to make that happen?

Emran Mian: The Treasury has done a lot of what we were hoping the Treasury would do: they worked really closely with us and prioritised this investment in the spending review. The key thing now for us to work on is the classic piece around accountability, which is a joint effort between ourselves, the Treasury and the Cabinet Office on the wider delivery of the

digital government road map. We also collaborate closely on the controls framework, particularly around major projects.

We are looking to continue work with the Public Sector Fraud Authority to ensure we get the benefit of their expertise on which data assets would be most helpful to tackling fraud and error, so that if Departments are not bringing those forward in early plans for the data marketplace and the data exchange, we ensure that that does happen. The other piece of work we have been doing together is ensuring that the next steps in improving the national fraud initiative data platform is done as well, and that is being funded through the transformation fund.

Q33 **Catherine McKinnell:** Thank you for what you have said so far, but I have to say that it all feels rather intangible at the moment. There is clearly no road map yet, no actual plan, no actual timeline and no actual targets that we have any visibility on. From the PSFA's perspective, what more do you need to see and what more should the Government be doing to work with you on these priorities?

Mark Cheeseman: If I step back a bit first, we have just talked about how we get the data quality and the access to it. Two points explored in the Report are how officials find the data and ensuring that the data quality is good. How do we get that in a really good place to support those tools, and how do we build capability in the community through the network so that people can access and use the data? The Public Sector Fraud Authority, and the wider counter-fraud function of 14,000-plus people, is doing work off the back of that to have the measured impact you are looking for.

One of the first things we do is to raise the profile of the issue. We are having the conversations on targets and on what people are doing. We have a published, functional strategy that says that using data and technology to deal with fraud is a priority. Every year, we publish lists of what Departments are doing under that priority—again, that is published. We use the transparency we talked about earlier to drive activity. We are building on the earlier challenges, and we are currently adopting a year-to-year process to deal with them. I note the challenge on that earlier.

I have already talked about how setting targets sets the incentives that you were talking about, including the incentive to do stuff on fraud, and to use data and analytics to have that impact. That work on setting the structure is part of the approach and part of the road map, and it is there and having an impact.

We also work alongside DSIT to help Departments to increase their capabilities. We have communities of practice alongside the network, and we release guidance and do training—all to try to increase the capability, because fraud work is increasingly technical and complicated. Making sure that people have the capability to use the data and the tools is an incredibly important part of that fraud work.

We also do things to make data sharing easier. We have the stuff on the data, and we have the Digital Economy Act legislation that we will talk about—it is talked about in the Report. We help Departments and advise them on how they do data-sharing pilots. We are in there to support them in doing that to build their capability.

Finally, there are cross-system products from both partners, including One Login. We run the national fraud initiative, and we run something called the internal fraud hub, which is to prevent people who commit fraud within the public sector from coming back in.

You are asking for the tangible benefits; since the Public Sector Fraud Authority was launched, it has brought £875 million-worth of benefits, roughly half split between local authorities and central Government. The benefits are there; I think the Committee's challenge is on how we go further.

Chair: Thank you very much, Catherine. That was a useful set of questions.

Q34 **Sarah Green:** I would like to look at the barriers that public bodies face in trying to tackle fraud using data analytics. If, for the sake of argument, we say there is a set of targets, what needs to happen to enable public bodies to meet those targets? Mark, what barriers can you identify that public bodies currently face? Why is it such a challenge for them right now?

Mark Cheeseman: There is a number of them. It is a very good Report and it explores them in quite a lot of ways. We have touched on some of them here—data quality is a barrier. The Government have a lot of data, and how you find the right data is a barrier.

It also requires investment. One of the things we say in counter-fraud is "problem, not product". It can be tempting to think, "I will put in this solution, which will solve anything," but fraudsters operate on the weaknesses of whatever is going on, so you really need to understand how they could operate to then understand the problem. That takes a skillset and, coming back to capability, that skillset is building. There are not widespread training courses on how you deeply understand fraud problems; those who work in the industry have learned it on the job. To do that on a wider basis, we need to scale up the great work that has been done in HMRC, DWP and other Departments through building that capability throughout the system, because there is a capability challenge as well. I have named a few of the barriers there.

Q35 **Sarah Green:** Some of the challenges sound quite basic, on the surface. The Report says in paragraph 2.19: "Public bodies continue to find it difficult and bureaucratic to share data…even though it is permitted under legislation." I was surprised to read that "public bodies do not know what data can be shared, or the information that data protection officers need to agree a data-sharing arrangement". On the surface, that sounds like quite a simple thing that could be fixed with a bit of clarity. Where does the responsibility for fixing that lie?

Mark Cheeseman: Public bodies find data sharing difficult because of the twofold challenges you have touched on there. First, where and what is the data? Secondly, how do I share it and what do I need? The Government have a lot of data—that is part of the challenge—and it is held in other spaces as well. For instance, I used to work in the Legal Aid Agency; there, I might need data from HMRC or somewhere else that is not in my organisation, so I would have to understand that organisation's data processes. We have just talked about some of the work that is being done, with the marketplace, to make that more visible across the system and to make that easier. That is one barrier, and it exists because Government is big and holds a lot of data.

Q36 **Sarah Green:** And complicated.

Mark Cheeseman: Absolutely; big and complicated. I will move on to why it takes a long time to share data, and those processes. First, to reassure you, challenge 7 in the Report—the bit that we own, about the Digital Economy Act—says that we should have standard templates and KPIs. We have taken that away and done those standard templates, and we will build those KPIs.

Q37 **Sarah Green:** So they now exist?

Mark Cheeseman: The standard templates exist. It was a good observation, and we will try to make that simpler. That is only one bit of the wider picture, though.

Why is it complicated? It is complicated because there is a broad range of legislation that plays into this space. There are different Acts with different requirements held by different Departments, and we need expert legal advice to make sure that we handle citizens' data appropriately. It is important that we keep the right balance between fighting fraud and keeping public trust that we are holding their data in the way that Parliament has laid down.

That requires exploring those different bits of legislation to then enable us to share. As the Report observes, that can be complicated and involve a number of different parties. If you are sharing data between three Departments, that is three organisations and three legal teams, all coming together to understand that and to explore the different legislation and how it interacts.

Q38 **Sarah Green:** That is really helpful; thank you. And thank you for using legal aid as an illustration, because—I won't lie—I am finding this quite difficult to follow because we are talking in the abstract, so a concrete example really helps. One thing that the Report refers to is that, quite often, data-sharing agreements are between two bodies, when, in the private sector, they are often multilateral. Will the platform that you were referring to earlier address that need, which I suspect the Report is identifying?

Emran Mian: Yes, that is what the platform is designed to do, so that any user of the platform can discover what data assets are accessible through

the platform. They can then see, from the information available to them immediately, which of those might be useful for their purposes—that might include fraud and error detection or other purposes—and then seek access to that data. Obviously, there still needs to be a legal foundation for that data sharing to take place—it needs to be legitimate and it needs to follow the rules—but it does make the discoverability of which data might help you a lot easier.

Q39 **Chair:** Permanent secretary, I need to return to a subject that we have raised so often in this Committee, both with other Departments and with your own, which is responsible for a lot of this. That is legacy systems in Government. There is an estimate, somewhere, that 28% of Government systems are legacy systems. The problem with legacy systems, as we have heard so many times in this Committee, is that, first, they are not supported, so they are being patched all the time; secondly, they do not talk to each other; and thirdly, they are more vulnerable to cyber-attack. And now we are hearing that they make it more difficult to root out fraud and error because they are not AI-compatible. What is being done to modernise those legacy systems on a fairly tight timescale?

Emran Mian: This is one important area in which the fact that we have had, on the whole, a good spending review settlement for data and digital is really important. Investment in updating these legacy systems is the thing that tends to get traded off when spend on data and digital is very tight, because Departments will often invest in the data and digital thing that deals with the service issue presenting there and then, rather than dealing with the legacy system, which feels like an important issue but not an urgent one. Therefore, one of the reasons why we focused so hard and worked so closely with the Treasury on ensuring a good settlement for data and digital was to be able to make this investment in legacy systems.

We are now doing two things to follow up on that. One is working with Departments as they go through their business planning processes for this spending review process, to ensure that the focus we want on legacy systems being remediated is actually there in the business planning decisions they make.

We are also going to develop a much closer approach to, if you like, monitoring and working with Departments on the delivery of their plans. We are creating dashboards to monitor what Departments are doing to improve service quality, what they are doing on the remediation of legacy systems, and whether they are delivering the improvements that their investment plans are supposed to deliver. This is a very big challenge, but I think we are now well set up to make some progress on it in the next spending review period.

Q40 **Chair:** My suspicion—I would be interested in your comment on this—was exemplified by Clive's question on Government Next Steps agencies: that there is possibly more legacy equipment in Next Steps agencies that is still nowhere near being addressed. The Department will address its main core systems, but there is a lot of legacy equipment in Next Steps agencies and ALBs that is not being addressed.

Emran Mian: Yes, there is. Some of these examples are public and well known. For example, one of the challenges around the system for booking driving tests online has to do with the fact that it is a legacy system. That is something that the Department for Transport is looking at as part of its investment plans and plans to improve that service. I do not know whether that is linked to it being an agency; I think that even core Government Departments have real challenges with their legacy systems. The dynamic that is playing out much more frequently is probably that Governments prioritise the new services that they can develop, rather than fixing the systems that they inherit.

Q41 **Chair:** I wonder, Mark, whether you should concentrate on this a bit, so that we have a bit more granular detail on where those bits of that 28% are. If we know where they are, people can at least start to concentrate on them so we can try to put it right. That is one of the limitations that you, Permanent Secretary, were alluding to in your plan.

The next limitation I want to come to is IT staff. The Report makes it clear that some of these analytics are being put in place but are not being properly implemented, because there are not enough staff to follow up on the inconsistencies that they throw up. That is just one of the aspects of not having enough staff. I think there are about 400 staff across Government with IT skills—I may have got that wrong, but I think the Report has that figure somewhere.

What is being done to address the shortages of digital staff in Government? We have heard previously that one of the restrictions on that is the amount that the civil service is able to pay according to civil service scales. What is being done to address this issue?

Emran Mian: It is an issue that we have recognised; we talk about it in the "State of digital government review". The Prime Minister has spoken about our ambition of increasing the share of civil servants who have data, digital or cyber skills to one in 10 by 2030, so a very significant effort is under way to drive up the level of capability on these issues. For example, we have started the new TechTrack apprenticeship scheme, for which we have had really high interest. We are now looking to place TechTrack apprentices across the full range of Government Departments.

That indicates to us that some of the challenges around pay are not at entry level. The challenges around pay tend to crystallise at more senior digital roles, which is where we find it more challenging to either recruit or retain people. There, it is absolutely true that the pay differentials between Government and the private sector are really quite high. We do have some pay flexibilities for people who have data and digital skills, so we aim to use those. One of the things that we do as DSIT is to make the case for what those flexibilities should be and we sign off on the cases that look to use those flexibilities, working closely with the Treasury. I think it still is often cited as a reason why people might leave Government Digital roles to work elsewhere, or why we sometimes find it hard—especially in senior roles—to hire in the very best people.

All that said, in the past few months we have seen some real successes in that respect—the combination of the fact that it is clear to people that we are investing more in data and digital in government, and the fact that not just senior officials but senior Ministers are really focused on this as part of the Government's reform strategy. I think that is being noticed by talented digital professionals. We have been able to hire in lots of very high-quality people in the past few months. For example, in my organisation, our new chief AI officer had a career in places like Spotify and Meta, but he wanted to come into government because he saw that there is a serious effort under way to improve where we are. Equally, the Home Office recently hired in a new director general to lead its data and digital efforts who came from a leading private sector organisation. So, in the past few months, there have been some positive signs that people are seeing that a change is afoot in Government, but the underlying challenge on pay is significant.

Q42 **Chair:** Listening to your reply, which is very helpful, it struck me, I wonder whether we could use fungibility with the private sector more, hiring people from the private sector on, say, fixed-term contracts to give the benefit of their expertise and to get public sector experience, but with them going back to their private sector firm after the contract period.

Emran Mian: Yes. We have lots of people in the Government Digital Service who have done exactly that. They have come in from the private sector, may not spend the rest of their career in the Government Digital Service and may go back out again to work in another organisation. I think we have to be very mindful of potential conflicts there and ensure that those are managed properly, but that kind of career model, where there is circulation between Government Digital functions and the private sector, is definitely going to be part of our skills mix. Alongside that, however, I think we need to grow talent within the service as well. That is why, for example, we have set up the TechTrack apprenticeship series. It is important to attract people in right at the beginning of their careers, because some of the digital jobs we do in government are complex, challenging and interesting, and I think they can be really good ways for people to build a career.

Chair: Thank you. That is really encouraging.

Q43 **Sarah Green:** I am keen to understand how you will make it easier for public bodies to fund and use innovative data analytics. We have talked about the road map, which we look forward to seeing, and the platform that you mentioned earlier, but I am keen to understand how their use will be funded and then how they are actually used.

Emran Mian: This probably goes back one of the points about where there is a clear business case for an individual Department or organisation to make the investment. For the majority, that business case will be there, because it benefits the organisation itself. When I think about organisations within DSIT or the DSIT family, an example is UKRI. UKRI is investing more in its counter-fraud efforts and laid out its new counter-fraud strategy, covering the period 2025 to 2028, at the end of last year.

That is exactly because the investments are good for the organisation itself, so it is making those investments.

Our role comes in when we need to create common bits of infrastructure, where it makes sense to create them once and where that is the most effective and efficient thing to do. That is why we are focused on creating the single register of data assets—that is a useful bit of infrastructure to create—and then to use that as the driving force for a platform that people can use to share data. Again, that is an example of something where building it once delivers benefits for others.

Q44 **Sarah Green:** I don't think I asked my question correctly, so I will ask it again in a different way—my apologies. I am keen to understand how that tool, or that data, can be used innovatively. Where best practice or an innovative new way of using that data has been identified by a public body, how can that be scaled up and rectified? Knowing that there is this shopping list of tools and data available is one thing, but using it in a really effective and impactful way is another. If I were a public body, how would I know that I can use this data in this really clever way? How would I know the use of it? I am not articulating my question very well, but I think you understand what I am asking.

Emran Mian: It is a really important point. For me, it was one of the really helpful things to take from the NAO Report. I thought that the NAO Report spotlighted some examples of that going on in a really helpful way. A lot of our colleagues across Government will have noticed those examples, and it will have given them ideas about things that they should be doing. That is absolutely how we want to use the data exchange. Once we have successfully done the beta and are rolling it out, we can show people what successful bits of data sharing have been done through it, and can then encourage them to learn from that.

Q45 **Sarah Green:** How would you do that? What would that look like?

Emran Mian: We have a network of chief data officers across Government Departments. In my organisation I have the Government's chief data officer, who we recently recruited from outside Government. She will convene that group of data officers from across Government Departments. Obviously, they talk about a whole range of issues, but they should be talking about really good examples of data sharing and what others can learn from the data sharing that some have already done. Mark may want to add some examples from the fraud sphere particularly.

Q46 **Sarah Green:** Before you do, Mark, how is that captured? That sounds like a group of individuals meeting. There are hundreds of public bodies, and they are not all going to be in the room for that, so I am keen to understand how that is captured and shared.

Mark Cheeseman: I can pick up a few points, if that is okay. I want to go back to your question about how it is easier to fund it. One of the things that we have—again, it is the only one that exists—is a leadership qualification for people who lead fraud functions. As part of that, we train them on making good cases—the best cases they can. That does not mean

that it will meet the criteria to be funded, but it will have the best evidence for that. That is based not just on examples in the UK but examples internationally—other countries' experience in that space. Guidance on that has been published by our partners in Australia, but everyone in the UK can access that and knows where it is online. That is easier to fund.

On easier to use and the sharing, obviously the network is very important. Earlier, I touched on our community of practice. You are right that not everyone is in the room when you have that community of practice, but we also produce packs and documents for those communities of practice, and they are circulated. Within the fraud function, we also produce guidance. We worked with our colleagues in Australia to produce a guidance set on how to do data and analytics fraud pilots. Again, it is the only one that I know exists from a fraud perspective—there are things on wider perspectives—and that is published. That guidance has more than 1,000 downloads, so we know it is getting there—people are using it and looking at it. It is that kind of structure.

The final end to that structure on our side is that we are building standards and qualifications for those working in fraud. That cycle then goes back in. Those learnings go into the training so that the next people doing those activities do them built off the learnings, experiences and knowledge of the people before, rather than starting again from scratch, as happened in the fraud space historically.

Q47 **Sarah Green:** So it is being embedded in the system.

Mark Cheeseman: Yes, absolutely. We are systematically embedding the learning in the system.

Sarah Green: Thank you very much.

Chair: Permanent Secretary, I must apologise to you, because you have not been before this Committee before. We normally take a break. I was hoping that for this hearing we would get away without a break, but we still have quite a bit to cover. I will take a break now for five minutes. It is 11.03 am. If we can be back here sharpish at about 11.10 am, we can hopefully have a relatively speedy race to the finish.

Sitting suspended.

On resuming—

Chair: Welcome back everybody, and thank you for your participation so far.

Q48 **Mr Betts:** The issue that we sometimes have in this Committee is the tensions between the centre, and the good ideas, guidance and examples of the best way to do things, and the Departments, which do not always follow those. The national fraud initiative has ideas about best practice and data sharing and matching, but lots of Departments just do not do it. Is that frustrating to you, and are you able to do anything to deal with your frustrations?

Mark Cheeseman: The national fraud initiative was set up in 1996 and brings data together from lots of different public bodies and private sector bodies to look for fraud and error in the system—predominantly fraud.

It was built starting with local authorities. Local government was where the real focus was when it was first built. It has branched out to involve more organisations, including the private sector and central Government. Sorry, it was local authorities and the NHS—the health system.

Increasingly, public bodies are using it—central Government bodies. We had six more Government Departments use it in the last iteration, and five more in the iteration before, so it is increasingly being used.

Is there more that could be done with it? Yes, there is potential for more to be done with it, but that has to be balanced. When an accounting officer or public body is considering using it, there are lots of different things they could do to deal with fraud, and they are prioritising their resource. They may consider that the return on investment from the national fraud initiative would not be as high as that from the activity they may do otherwise.

There are parts of it that we would encourage more use of. Part of it looks at multiple working—if a person is potentially working in lots of different public bodies. Of course, the more organisations that are in that, the stronger that check is.

Q49 **Mr Betts:** You mentioned that local authorities have to use it—they have no choice.

Mark Cheeseman: Under the legislation, because that was how it was created. Originally, it was created for local authorities, and the whole thing was created with the legislation so that they would use it.

Q50 **Mr Betts:** So local authorities are mandated, but Government Departments and arm's length bodies do not have to use it. However, it is clear from the system that it benefits not just the Department that decides to engage in the data sharing, but other Departments as well. A Department may take a decision, as you said, because it thinks that something else is a higher priority, but that affects the working of another Department that would benefit from data sharing. Is there not a need for the centre to start mandating this and saying, "You will do it"?

Mark Cheeseman: There is a nuance there. There may be an argument for more mandation from the centre of data sources that should come in, which is what makes it richer, as you said. However, a wider mandate that says, "You have to use it," is less strongly arguable.

Also, because it is designed around local authorities, we collect a lot of data from them. As to whether those same sets of data would be as helpful in the national fraud initiative, I do not think that is proven; local authorities have very similar risks, some of which are quite different to some of the risks that public bodies face. Again, I go back to what I said

earlier: you would generally drive it from your risk, rather than just adopt a product.

Q51 **Mr Betts:** Right, so mandate that Departments or bodies have to put in their data and share it, but not necessarily use it.

Mark Cheeseman: Yes, there is an option to mandate putting in data, rather than using it.

Q52 **Mr Betts:** So why is that not done?

Mark Cheeseman: Currently, the legislation that mandates it dates back to when it was created, and it has not been amended to bring in other public bodies.

Q53 **Mr Betts:** No, but they could be brought in by the Treasury saying, "You will now use it as part of your spending review. This is a requirement."

Conrad Smewing: I think what Mark is saying is that there is a distinction between maybe central Government bodies which have data that would be very valuable to a large number of other people, and mandating all central Government bodies, most of whom do not actually have that sort of data.

To take an example at one end of the spectrum, it probably would not be sensible to mandate the Office for Budget Responsibility to engage in this fraud initiative, because its payments are essentially to only a relatively small number of people, and it does not have any interaction with the public and businesses. However, if there are central Government bodies that have valuable datasets that are not in there, you could look at using more sticks, or more mandation, on those. This was a recommendation of the NAO Report, which I think we will look at seriously.

I think what Mark is saying is that you would not necessarily go straight to blanket mandation to all bodies that we have, for instance, for producing whole of Government accounts. It is more about which bodies are not taking part, where it would be very valuable for them to do so.

Q54 **Mr Betts:** Should you not turn it on its head and say that Departments should have to do this, unless there is a good reason why they should not?

Conrad Smewing: I think it is the question of the very large number of public bodies for which there might not be a good reason. How do you most efficiently get to those that are not currently using it, where it would be very valuable to get them to?

Q55 **Mr Betts:** You just tell them, don't you?

Mark Cheeseman: It is something that we should consider, but I think a blanket mandation—as Conrad is saying—may be sub-optimal. I think there may be some more nuance around it.

Conrad Smewing: But as you are saying, there are a number of ways that you can mandate it or make it a strong requirement for different central Government bodies. You can link it to funding, as you mentioned,

and there are other ways, such as linking it to accounting officer letters and responsibilities. We want to look at whether there are significant gaps where bodies are not using the NFI, and whether we should have more teeth in forcing them to do so.

Q56 **Mr Betts:** I am just getting the feeling, "It's a nice idea, and we'll think about whether we should do it." If this has real benefits—clearly the centre believes it has benefits—should the centre be saying that the benefits are so great for the whole of Government that everyone should be engaged in this?

Mark Cheeseman: I think we should weigh it up carefully, like all things. For instance, I would want to look at what benefits they are getting from the analytics work they are already doing. Would the national fraud initiative supplement that? Departments have grown up individually and looked at what data would help them manage their risks and what they want to do.

We are giving you a nuanced picture, because I think it might not quite be one size fits all for Government Departments, which are less similar than local authorities were when the national fraud initiative was created under the Act.

Q57 **Mr Betts:** There are obviously issues around confidentiality of individuals' information. The public probably want to do both things, don't they? They want to know that their personal information is kept confidentially and properly by Government. At the same time, they want to help with the challenge to defeat fraud. Clearly, there are issues to be dealt with when data sharing is done between public bodies. You mentioned the standard templates that exist: who actually manages those and enables Departments to use them effectively?

Mark Cheeseman: The standard templates I talked about were in response to the challenge in the NAO Report about the Digital Economy Act data-sharing process. We produce standard templates for that. They are managed by the team that sits within the Public Sector Fraud Authority, and Departments that are using the Digital Economy Act would use them working with that team.

Q58 **Mr Betts:** We hear from the NAO Report that it can take weeks, sometimes months, for agreements to be formalised. If there is a standard template, you do not have to reinvent the wheel every time you do an agreement, do you?

Mark Cheeseman: You don't, and it should bring that down, but I would say a few things on that.

Pace is important in order to have quicker impact, but you can do things too quickly in fraud management. If you will excuse me straying into metaphors, I talk about it as "doing the decorating". Basically, when I do some decorating, I spend a lot of time prepping the walls before I put anything on them, to make sure it works.

It is the same when you use data analytics: you spend a lot of time

understanding the problem, the data you are going to use and its weaknesses. Sometimes the data you are going to use has not been collected for the purpose for which you might need to use it, and you do not want to find that out when you have done the data share and you are using it. Actually, in some of that, the more time you spend up front understanding the data before you use it—before the data sharing goes live—the better the results that will come from it.

There are other aspects as well—for instance, data security and legality. Are we okay to share this data? That should be checked thoroughly. Will the data, when it is shared, be held securely, as the taxpayer would expect, in line with the legislation? That needs to give assurance. For instance, the Public Sector Fraud Authority has a data governance team that does that for everything we are involved in, to make sure the piece of confidentiality that you raised is kept.

I agree with the challenge in the Report. We should look to do it faster, but I would not want to be coming here saying that we are doing it in one day, so it is great. It is a balance between pace and integrity.

Q59 **Mr Betts:** But time taken to do it is not merely a delay to get something good in place. It also takes a lot more effort from the people involved—

Mark Cheeseman: Yes.

Mr Betts:—when, actually, there should be experts at the centre, who understand the process, the procedures and the standard template, saying, "This is how you can do it," to Departments. Is that what you do?

Mark Cheeseman: We are building those standard templates, but those standard templates then tackle discrete problems that will have their own nuances around those areas and systems that you need to understand. So it is that balance that I am talking about.

Q60 **Mr Betts:** And you provide that advice on the standard way of doing things, do you?

Mark Cheeseman: We provide advice to Departments, with the resources we have, on how to do it, yes.

Q61 **Mr Betts:** Is that when they come to you and ask for advice, or do you proactively go and sell your services?

Mark Cheeseman: We have a community of practice that local authorities, as well as central Government public bodies, come to. We have a series of functional leaders who lead as well. We talk to people and tell them it is there. However, the choice is on the Department whether they want to engage with us, and some have the capability to do it without us as well—so it is a balance.

Q62 **Mr Betts:** You just mentioned the costs involved in participating in the NFI. What are they?

Mark Cheeseman: The costs for the national fraud initiative?

Q63 **Mr Betts:** Yes, the cost to the Departments involved in engaging—

Mark Cheeseman: The cost to a Department to engage in it? The cost to be involved in it is, I think, referenced in the Report, so I will use the number from there.

Chair: Figure 5 on page 29.

Mark Cheeseman: It is £1,265, but there are different aspects to the national fraud initiative as well. You may use different parts of it, like our AppCheck, which you may pay an extra fee for. It is in the thousands of pounds. There are additional costs to a public body to use it, because they have to prepare their data to put into it and send their data in to it. We also touched earlier on the fact that what the fraud data analytics produces is indicators that something might be wrong, not a, "This is definitely fraud." So there will be costs to follow up the matches that come out and to sort the positives and false positives.

Q64 **Mr Betts:** You mentioned local authorities earlier. They hold data about people claiming housing benefit, to a degree, and council tax support. That is important and it matches across what the DWP can be doing. It is not just about local authorities in isolation, and therefore it is easier for them to do data sharing, because they data share with Government Departments, which is really important.

Mark Cheeseman: They do, and there is a lot of data sharing that goes on between local authorities. As I said, a number of public bodies already use the national fraud initiative. It is not that no one is using it and that it is not used across the system. A number of pilots for the Digital Economy Act have been with local authorities using central Government data, so there is quite a lot of interoperability going on between those two sectors.

Q65 **Mr Betts:** We also have NOVA, apparently—another alphabetical jumble of letters. Again, NOVA is something that is there for Departments to have if they want, or is there any requirement to use the initiatives in it?

Conrad Smewing: NOVA is essentially a standardisation of some of the real nuts-and-bolts plumbing of finance systems in the public sector—standardisation of data and, I think, also some standardisation of processes. It is helpful for a number of reasons, but it helps support interoperability and the shared services strategy. It is also helpful in fraud and error, because the standardisation of data to allow easier matching is an important part of making that successful. So that's what it is. As I say, it is helpful in this context because it is doing the basic nuts-and-bolts plumbing to help different public bodies share data on payments and that kind of thing.

Q66 **Mr Betts:** That is helpful, but how far does the Public Sector Fraud Authority work to ensure that the greatest benefits of these processes are realised?

Conrad Smewing: Mark should come in on this, but the Public Sector Fraud Authority are already working with the people who do the NOVA finance system. They have fed in the work that they have already done, to

make it helpful. I think there is a question of what more can be done on standardisation via NOVA. That work is ongoing at the moment.

Mark Cheeseman: NOVA references the fact that fraud risk assessment, which we have talked about already, is an important part of the processes, so that is built in, along with the structures we have for fraud risk assessment. It also identifies control points where fraud and error is most likely to happen and that should be considered and looked at. Again, it is a helpful lever as part of the standardisation of processes for when fraud and error is considered. We have touched on the standardisation of data, which is hugely helpful for data sharing as well. A good observation in the NAO Report is that there are opportunities to make that even richer, and we are already working together to follow up on that recommendation.

Q67 **Mr Betts:** To give a nice simple example that we can all understand, hopefully, even MPs: when we as individuals go to our banks and use our apps and transfer money to some other person or organisation, we have to put in not merely the bank account that we want to transfer to and the sort codes but also the names so it can be cross-checked by the bank very quickly. I understand that is best practice in government, but it is not required. You have people transferring large sums of money without properly double-checking that the account and the organisation or individual match up. Why?

Conrad Smewing: I am not sure whether that is required. I would have to take it away and look at it. I don't know whether the NAO has the facts on this. My understanding is that the processes that are being standardised through NOVA do build in the kind of checks that you would want to have. Whether that is all the checks that occur in the banking system I don't know; I would have to take that away.

Q68 **Mr Betts:** It would be helpful if you would, because it just seems, again, a very basic requirement that you do not pay money over unless you are sure that it is going to the right place.

Conrad Smewing: I am happy to take away whether that is exactly what the position is, because it's a bit too technical for me.

Mr Betts: It would be helpful to follow up. Yes, it is a low-level requirement at one level, but actually it is a fundamentally important one. If we could come back on that point, that would be really useful.

Q69 **Sarah Green:** I would like to turn to a slightly different topic: transparency around the use of AI. Understandably, concerns are expressed about transparency and the fairness of using data analytics to tackle fraud and error, and I think the NAO Report references officials saying that meeting the requirements of transparency can be difficult without revealing too much, which makes life easier for fraudsters. I would like to ask the whole panel, if I may: what you are doing to assure the public that data analytics are being used appropriately by Government, and what safeguards exist at the moment?

Emran Mian: I can come in on this first. You are right to say that we expect there to be transparency around the use of algorithms, AI and machine learning in decision making. We have, I think at the last count, over 100—something like 120—records that are now part of our central recording of algorithmic transparency records.

Q70 **Sarah Green:** Is that the algorithmic transparency recording standard?

Emran Mian: Yes, that's right—the ATRS.

Sarah Green: That's a new acronym on me.

Emran Mian: Yes, it's a proper mouthful. I didn't attempt it, but you pulled it off—thank you! That is not the full total of the records that could be created. On some of them, we are in discussion with Departments about getting it recorded—

Q71 **Sarah Green:** It is not yet a complete list.

Emran Mian: It is not a complete list. I think we are pretty confident that it is the majority, but it is not a complete list. One of the challenges that we definitely have with Departments when we are having this conversation is about not wanting to reveal information that may then help someone who is seeking to commit fraud. We have provided guidance on this point and we are really clear in the guidance that accompanies the algorithmic transparency recording standard that organisations can withhold information that would create fraud or, indeed, security risks, which is another issue.

Q72 **Sarah Green:** Who makes that decision? Do they make that decision themselves?

Emran Mian: It is the Department that makes that decision, on the basis of the guidance that we provide. We do expand, in the guidance, on the risk of people gaming the tool. That is something that Departments should be thinking about; it is an active concern. Are we quite getting that balance right? I think equally there would be people who would say that we do not have enough records published yet and more records should be published, but we are trying to strike a balance between getting the appropriate records published and not giving away information that would help fraudsters or, indeed, create security risks.

Q73 **Sarah Green:** Is that an active piece of work taking place at the moment and are you working to a specific timeframe, or is it a never-ending project because tools constantly—

Emran Mian: Yes, it is a never-ending project, because some algorithms would be retired because they became outdated and so you would want to replace them. Equally, new ones are being added all the time because Departments are expanding their use of AI and machine learning. It will be an ongoing piece of work.

Q74 **Sarah Green:** But the ultimate responsibility for that hub rests with your Department?

Emran Mian: That's right.

Mark Cheeseman: Let me say, coming in from the fraud management side, that transparency is absolutely key, but over-transparency—to probably misuse a phrase—would be really damaging, which is what we have explored. If we were to say, "Every single lock and key", we would have a very capable and committed adversary, we would be giving them a guidebook on how to defraud public bodies and public money. I would personally advise against that.

There is a balance to be made. You talk about what analytics you use and let members of the public know how their data will be used. However, I would not advocate for publishing every single data-share check that goes on. I would especially not advocate for talking about what does not go on—because it has been decided not to—because you would then give a guidebook on how to defraud the public sector, and we have a capable and committed adversary.

However, we do a lot on transparency. I can talk specifically, because we run tools about what the Public Sector Fraud Authority does. For instance, the data shares we do through the Digital Economy Act 2017 are published and there is a register that lists those—where the data is coming from and what it is being used to do. That is really important. We also publish a code of practice, which we must abide by and work under. Looking at the national fraud initiative, we again publish a code of practice for that, which we must abide by and act in accordance with. There are data privacy notices up front for any data that goes into the national fraud initiative, which tell the person interacting how their data will be used and what legislation it comes under. There is real transparency on that. As you would expect, all of these things are overseen by the Information Commissioner's Office as well.

We have another tool that we have not talked about today. We have talked about how we use data to find fraud, but we also use technology and AI to get better at the process of managing it. We have something called the fraud risk assessor accelerator tool, which makes it quicker to do fraud risk assessments. That operates with an algorithm and that algorithm is published in line with the expectations of DCIT and Government. We do a lot of that transparency work.

Q75 **Sarah Green:** Do we currently strike the right balance between protecting individuals and allowing public bodies to identify fraudulent behaviour? Do you think that anything needs to change?

Mark Cheeseman: It is a good question. The balance is roughly right, but you must continually review it because the technology is changing, what we are doing is changing and what our capable and committed adversary is doing is changing as well. We should be alive to all those different aspects and keep it under constant review. To your earlier question, it will never be done; there will be a constant cycle of doing this and trying to best strike that balance.

Q76 **Sarah Green:** How do you do that?

Mark Cheeseman: You review. When you do new data shares, you look at those and when you use new things, you look at them and try and strike that balance. We share practice around. When creating one of these products we do not start from a blank but look at what others have done and challenge that and whether they have struck the right balance. It is something that the counter-fraud profession, which I look after, talks about. We are here to act for the public, so it is very important we have their trust.

Q77 **Sarah Green:** Are you comfortable that, at the present moment, broadly we have the balance right?

Mark Cheeseman: Yes, the balance is broadly right at the moment.

Q78 **Chair:** Following Sarah's line of questioning, we know, for example, that DWP had to withdraw two of its data analytic fraud detection systems because it was worried about the ATRS. In particular, some of these systems can disadvantage certain groups. Is enough attention being paid to this area before any system is implemented? Does it go through some form of scrutiny to see whether it passes the ATRS tests?

Mark Cheeseman: I cannot talk specifically to the DWP example but I will talk more generally. Before we do a system, we make a data privacy impact assessment and consider those aspects. I talked earlier about our data governance team at the Public Sector Fraud Authority. It works with our people who are using the analytics to do that and ensure that that is done as thoroughly as possible. When you then start using the system, you start seeing what it is producing and the trends that it is producing. What is important is that not just that you do it up front but that you then continue to do it.

Q79 **Chair:** Allied to that question: when any Government Department introduces a new system, is there an obligation before introducing it to look at how it could be designed to remove the possibility of fraud and error?

Mark Cheeseman: Every new initiative created in Government requires an initial fraud impact assessment. That is again a change since our last Committee in that that is now widespread. In fact, the Public Sector Fraud Authority and the Treasury look together at initial fraud impact assessments to consider that. When new initiatives are created that is up front there as something that we do.

Q80 **Rupert Lowe:** I think this is a very interesting piece of work, and I came along today to learn as much as anything. People talk about the digital revolution, and it is making a huge difference everywhere. I was really intrigued as to whether you have been to talk to some private sector businesses that face the same challenges that the digital revolution brings, and whether you have discussed with banks or businesses such as Revolut, which run their businesses on a very digitalised model and must face the same risks of fraud. You cited the two cases of HMRC and DWP, which seem to be the main sufferers of this. You mentioned error, and I

am intrigued to know, of the huge £55 billion to £80 billion leakage that appears to have been identified by the NAO, what proportion of loss is from error.

I run lots of businesses. We face and suffer from this in those businesses, but we have managed to deal with it. The upside of the digital revolution is that you can cut staffing levels massively, and one of the reasons for problems is staff turnover. The public sector suffers far higher staff turnover than elsewhere. To what extent do you think the vast staff turnover, and vast numbers of staff, are contributing to the leakage that appears to be happening? I have posed a series of questions, having just been listening to this session. Most importantly, have you been to talk to the private sector to learn how it is dealing with this? It is almost equivalent to the train and the way in which it revolutionised travel. The digital revolution is almost now revolutionising the way in which businesses, and obviously therefore Government, run.

Mark Cheeseman: Yes, absolutely. The counter-fraud industry, in which I sit, is an industry across sectors. We talk to the private sector a lot about the challenges it faces. I personally have been into the banks, and they have shown me how they do it. I have been into insurance companies, and they have shown me how they do it. I have had roundtables with insurance companies to see how they do it. We have a common adversary, so we spend a lot of time exploring. Some of the tools that we run, such as the national fraud initiative, also provide services to the private sector to help them manage their challenges. We use the data that the Government hold to help to tackle that wider problem as well. A lot of collaboration goes on, and some of the people we have in the Public Sector Fraud Authority have come from private sector backgrounds. We have an independent advisory committee, and people from banking and other areas sit on that. We work with them a lot to explore it because we have a common adversary, and we will continue to explore how we can learn between those two sectors and other sectors as well.

Q81 **Rupert Lowe:** It is a vast amount of money. We are seeing the private sector being taxed—we are seeing taxes on farms, we are seeing taxes on small businesses and we are seeing business rates going through the roof—but that almost pales into insignificance when you look at the numbers we are talking about here, so it is absolutely crucial that we get it right.

Mark Cheeseman: We have talked a bit about the impact the Government are having on that, including over £7 billion from taking action on fraud and error across the system.

Rupert Lowe: Maybe you should go and have a chat with Elon Musk at X. He managed to cut 80% of his staff, and it seems to me that his platform works better now than it ever has, but there we go.

Q82 **Chair:** I have a mixed set of questions to sweep up. The first one is to you, Mark. Paragraph 2.5 on page 25 relates to the Digital Economy Act 2017 and shared data. What the paragraph, and figure 4 below it, tells us is that there are only four pilots out of 28 that have progressed to

becoming business as usual, or in normal use. I am just wondering how the Digital Economy Act is working, or not.

Mark Cheeseman: I feel that it certainly is working, and I would point to the benefits that it is producing. The report that was published by Government stated that it produced more than £134 million of audited benefits in reducing fraud. We are up to around £80 million since then, and that was it was two years ago that we published that report, so it is certainly having an impact, and other countries look to that legislation and ask, "How can we do more of that?"

The challenge is that fewer of these are going to business as usual. There are a few reasons for that. Some are that it is used as a one-off thing: we have detected what we want to detect; we now move away and prioritise elsewhere. We have seen that as a behaviour in using the Digital Economy Act. The other is the challenge, as we talked about earlier, of scaling up these things. It requires significant compliance resource or investment, and the assessment of the public body at the time has been that, for the benefits it is realising, there is not a strong enough case to turn that into business as usual.

What we are seeing, though, is an increase in the number that are starting to become business as usual, and I would happily write to the Committee to show you that trend as that is happening. That may be indicative of the maturity in the system as it is gathering pace.

Q83 **Chair:** Just to stick on that page, with the library of toolkits that builds on the PSFA post-event toolkit: public sector bodies find it difficult to share data under the DEA, whereas this library of toolkits may help. Do you want to comment on that?

Mark Cheeseman: Yes, it is a good recommendation. It is in line with the standard templates and pieces like that, about how we actually make it easier. We are already taking that forward. It was a very helpful observation.

Q84 **Chair:** Reading the Report, time after time it says that preventive measures are better than retrospective ones because, clearly, you have prevented the fraud and it has not happened, but it seems that more of the systems are currently using reactive rather than preventive ones. How are you moving from one to the other?

Mark Cheeseman: It is an active part of our strategy to encourage prevention. The targets we agree with Departments are "recovered" and "prevented"—the things that have an impact on the taxpayer. That is what we are looking at. As I say in our strategy, it is to move to prevention. That is layered throughout our guidance and the work we do with Departments.

It is, however, challenging, and I think it is worth me sharing some of those challenges briefly, if that is okay. It is more difficult to measure prevention—much more difficult. But, again, that is not something where we have gone, "Okay, it is more difficult to measure prevention. Move on."

We are just about to publish guidance with the Five Eyes on the leading practice across the US, Canada, Australia and New Zealand for measuring and recording prevention. That is imminently going to be published, and we will then use that in the Government to try and get better at measuring prevention.

Preventive tools can also be more expensive to implement: if I am implementing a detective tool, I can bolt it on to the thing; if I am implementing a preventive tool, I have to redesign the process and the system around it to insert it up front, so that makes that case we talked about more expensive and more invasive. That can then change the dynamics of the business case when trying to move to prevention, so we have to work on that feature of the challenge as well.

I would also highlight that the temptation can be to think of prevention and detection as opposites. They are not; they are on a spectrum. Part of the journey is coming to earlier detection so that less loss is realised. For instance, in the Report we talk about Project Athena from the Department of Health and Social Care largely as a detective tool, but around £60 million of prevented benefits have been audited as well, because doing earlier detection also brings prevention.

Q85 **Chair:** Permanent Secretary, this will probably be the last set of questions—I am afraid it is a set of questions. I make no apology for going back to staff, because without good staff you cannot do all this stuff. Paragraph 2.21 on page 37 tells us, in the middle bullet point, that we "spent £14.5 billion on digital contractors in 2023" but "GDS told us that, in April 2025, 5.5% of civil servants had expertise in digital…GDS is working to increase this proportion of digital, data and cyber professionals to 10%." That is a massive target to go at, not only in raw terms. We have been around this already in the Committee, but I am wondering now, having thought about it, whether the civil service is agile enough. As we move more functions towards digital, some of the traditional functions ought to go. I wonder whether resistance in the civil service to getting rid of those traditional functions and moving them into digital is part of the problem. It would also free up more funds.

Emran Mian: I think there will be two things that we do as part of moving from 5.5% to 10%. I should say that some Departments are obviously already well on the way to 10%, and some are above it. As you would expect, because of the things that we do, my Department is well above it. We are working particularly intensively with the Departments that are quite a long way below the target, because that will bring them up. I expect that two different things will happen as part of bringing them up. One will be that they will make exactly the switch that you describe, and do more things digitally that they are currently doing in an analogue way. As a consequence, they are going to need more digital skills, and probably fewer people, as you suggest. The other thing that will be going on here is that some of the digital functions are currently outsourced or done by managed service providers, so the change that we will see is that some of those will be brought into Government Departments, which provides better

value for money and means that we have more people within Departments with that set of digital skills.

The final thing I will add is that I absolutely agree that there is an attitude and orientation that often comes with people who have these digital skills, which is that they work faster, they are more agile, and they are more willing to try things and see if they work rather than waiting until there is a perfect solution—there is much more iteration in terms of how people work. They are usually more outward facing, and especially if they have come from a private sector background, they are used to working with a wider range of people. All those things are really positive for the culture of the civil service, as well as meaning that we will have a better set of digital services.

Q86 **Chair:** Thank you for that. Partly sticking with personnel, but moving on to the machinery of government, I understand that your Department—it was mentioned at the beginning of the session—has abolished the role of chief digital officer. I am worried about the transfer of all this digital stuff from the Cabinet Office to your Department, and whether your Department will have sufficient clout among all other Government Departments to start implementing some of these changes. Why has that post been abolished?

Emran Mian: I am glad to have the opportunity to clarify that. We used to have a single person at director-general level who led all the digital work that was in the Government Digital Service. Given our increased ambition on digital and data, rather than having a single person who is styled as the chief digital officer, I now have two directors general who lead on two different parts of the agenda. Broadly speaking, I have a director general for digital products, which are the things that the Government Digital Service builds and runs itself. I also have a director general that I am calling the director general for digital transformation, whose role is to work on the architectural things that support other Government Departments to deliver their digital programmes. That includes some of the stuff that we have talked about today on data, the digital profession, and the use of AI across the civil service. What I have actually done is gone from a position where I had a single director general who was looking to lead all of that, to two directors general to reflect the increased ambition. Commensurate with that, we are increasing the overall staffing on digital and the overall level of digital leadership.

Q87 **Chair:** I think that is a perfectly reasonable explanation, but the Committee has recommended—and had its recommendations accepted—that every Department should have a very senior digital information officer, in a very senior team, and at the same time have the same skills on the non-executive board. Is that something that you would push for? I understand that your Department, which plays the major role, needs two people to do that—that is reasonable—but in other Departments, particularly where they are not making so much progress, do they need a senior person and a senior person on the non-exec board?

Emran Mian: I expect that is right, and the big digital delivery Departments are all more or less in that position. DWP has a director-general-level person who leads on digital and sits as part of the top team. The same is true at HMRC and at the Home Office. When you look at all the major digital delivery Departments, this is now becoming the case. There are other Departments with smaller digital services, or where the bigger digital services are run by arm's length bodies rather than by them directly, which do not have that role at director general level. Instead, it will typically be the chief operating officer who is a director general and has a responsibility for digital, and then they may have someone at director level who is responsible for those digital functions.

I think your point on non-executives is right as well. Again, I believe that the key digital delivery Departments now all have someone on the board who has experience in digital. That is certainly true for my Department, and for some of the other big digital delivery Departments that I can think of. The other thing we have started to do is have all the non-execs across Government who have digital experience meeting together as a group, to share what is going on in their Departments and the issues and challenges that they face in improving the digital functions.

Q88 **Chair:** That is a perfectly reasonable answer. The only thing in it that I would slightly take issue with is that the need for digital change is probably just as great in a small Department. Therefore, by emphasising the need for that change, they probably just as well need a chief digital officer at that senior level.

Emran Mian: Yes, I think there does need to be clear senior leadership for the digital function. Different permanent secretaries will make different judgments as to exactly what grade that is held at, but the overall trend is that people recognise that and the roles are being held at a more senior level than was previously the case.

Q89 **Chair:** When you gave the job description of those two senior directors in your Department, you did not mention which of them actually has the counter-fraud function within their remit.

Emran Mian: The counter-fraud function for DSIT as a Department is held as part of our chief operating officer portfolio. The data function is under the DG for digital transformation. I talked about the work we are doing with other Government Departments to improve the register of data assets and their quality, and to create a single service where they can be accessed on a shared basis—all of that sits with the director general for digital transformation.

Q90 **Chair:** Okay. Could I take you to paragraph 3 on page 4? There are three big functions. Mark and the PSFA are shared between two Departments: the Cabinet and the Treasury. That is the Government counter-fraud function. The Government digital and data function is with you at DSIT, as you have just said, Permanent Secretary, and the Government finance function is with the Treasury. But they all have bits in relation to this policy. I wonder whether your Department is strong enough to bring all

this together to be able to translate it across Government.

Emran Mian: On the wider data and digital piece, yes, I think we are. I suggested some of the proof points of that earlier, such as the really successful partnership we had with the Treasury on ensuring a good spending review settlement for data and digital spend. There is also the work we were able to do across Government on exemplifying why and how the Government need to get better at data and digital, which was the "State of digital government review" that was published last year. You will judge whether the road map that we are hoping to publish, which is the reform plan, meets the ambition that we set out a year ago. I am confident. There is a lot more to do, and we need to keep focused on this and keep strengthening the team, but I think our early proof points are positive.

Q91 **Chair:** I know this is an invidious question. Can you be reasonably confident that the road map will be published this month—or in other words, in the next fortnight? I suspect that will affect the timing of our report.

Emran Mian: My hope was that it would be published before Christmas. I am very much looking forward to publishing it this month.

Chair: Good. Thank you very much.

Q92 **Blake Stephenson:** I am interested in asking some questions about the legislative framework; some of the responses to questions that Sarah asked piqued my interest. My constituents—all our constituents—would be horrified to know that in 2023, £55 billion to £81 billion of their hard-earned money was lost to fraud and error. They might also be disappointed to see that there is a £26 billion spread there—we don't really know how big the issue is. In the last two Budgets, the Chancellor has raised tax by £66 billion. Our constituents do not want to pay tax for it to be wasted by the state.

It is really important that we have the right legislative framework that gives you the tools to do what you need to do to bear down on fraud and error. I want to understand whether you think the legislative framework is adequate, fit for purpose and flexible enough for you to deal with the issues on your plate. Are there any recommendations that we could take forward to improve the legislative framework for you?

Mark Cheeseman: Let me first pick up on a couple of points. To reassure the Committee, and people more widely, the £55 to £81 billion figure is not the loss; it is the level. It is a gross figure, and action is taken on that by the Departments. It is still large, and I am not shying away from that, but I wanted to give clarity on that point.

In terms of the legislation, it is a decision for Parliament, Ministers and the Government as to what legislation is taken. The legislation that we have and that we use has a lot of strengths. The Local Audit and Accountability Act, which drives the national fraud initiative that we have talked about, means that we can mandate local authorities and NHS bodies to provide data. We can use that data because of the legislation, and it finds millions

of pounds worth of fraud and error and reduces it. There is strength in that. The Digital Economy Act, which was introduced in 2018, means that we can share data that we could not have previously. We have a mechanism where, if data cannot be shared because of other legislation, we can then say, "Now we can." There is strength to the legislation that we have. I talked about the international community, which we form part of and bring together. They actually look to the UK's legislation and ask how they can move towards this kind of approach, where there are avenues to share data more freely. It is seen as good practice.

The legislation has limitations, and there is always a balance being struck between the issues we talked about more widely. I am happy to give some specific limitations if that is helpful for the Committee. For instance, the Local Audit and Accountability Act cannot be used for live investigations. It can be used to look for and prevent, but if a live investigation is going on we cannot use the data that we hold to help that investigation. That is because the Digital Economy Act, when it was created, more specifically defined "detect, prevent, investigate". That is the legal model now used, but the legislation is older and does not have the word "investigate" in it, so it cannot be used for doing that.

The second thing that it does not allow is profiling for individual behaviours. I will explain that, because it sounds quite big: if we find that someone has committed fraud using data from the national fraud initiative, we cannot use that as an indicator the next time, when they are back in the system. The legislation did not allow, when it was written, for that to be done. It is a standard tool used in other industries where someone has committed fraud, to be an indicator that they may do it again. We use it in other tools that do not use that legislation, but we cannot under that legislation; there are limitations.

To preserve and make sure that data is managed as well as possible, under the Local Audit and Accountability Act we have to get rid of the data after a few years. After every two-year exercise, the data—all data—is removed and destroyed. As a fraud practitioner, we could do more if we kept the known frauds in the data. If you look at other industries, they have more historical data on what fraud has occurred, which they can then use to train models to understand what to look for in the system. That is a limitation of the legislation that we currently operate under.

Finally, we are limited to data matching under that legislation. One of the techniques you could use is outlier analysis. You would get all the data together and ask where the outliers are. The legislation does not enable us to do that, so there are limitations to the legislation, but it does enable us to deliver a lot of benefits.

Q93 **Blake Stephenson:** One follow-up: if we were to fix all those limitations, how much more of this error and fraud do you think will be detectable, which of course would then limit the need for the Chancellor to raise taxes in the future?

Mark Cheeseman: I cannot answer that question now. I would like to give you an educated answer.

Q94 **Blake Stephenson:** I think it would be helpful if you gave some thought to that and maybe wrote to the Committee, because there could be some really practical recommendations that we could make, in terms of changing legislation, which would help you to bear down on error and fraud, and in turn reduce the burden on our constituents through tax rises.

Q95 **Chair:** I suspect it would a guesstimate because it is quite a lot of work.

Blake Stephenson: I am sure it would.

Mark Cheeseman: As we have talked about in this Committee already, the legislation is one dynamic. Another is the capability, and there are other dynamics that we have explored today.

Q96 **Chair:** Indeed, Mark, the Local Audit and Accountability Act 2014 limitations are widely set out in paragraph 2.26 on page 40 of the Report, but I am a bit surprised to hear you say that the limitation of keeping data is two years. After all, any of us who run a business know that the Inland Revenue requires us to keep records for at least six years. Why are the Government allowed to keep those records only for two years?

Mark Cheeseman: Because that Act—and it is a bit longer than two years; the exercise lasts two years and once we have finished it, we need to not keep the data—explicitly says that that is how that data should be managed by the national fraud initiative.

Q97 **Chair:** I get that, but just to be very clear in your answer to Blake, are you saying that that is a significant limitation, which, were it extended, could enable you to investigate a considerable, big chunk of fraud?

Mark Cheeseman: Extending it would enable the national fraud initiative to do more work looking at historical trends and have a bigger range of data by which to use the modern tools to look for fraud.

Chair: That is really helpful, and a good note to end on. I thank all our witnesses very much; you have given us a lot of very interesting information this morning. The uncorrected transcript of today's proceedings will be available in the coming few days, following which we will carefully consider your evidence and produce a report with recommendations, which we would ask you in turn to consider very carefully and see whether you accept them. Thank you again for your time; you are all busy people, but I think we have moved this whole subject on today, so thank you very much indeed.