



Work and Pensions Committee

Oral evidence: Fraud and error in the benefits system, HC 1082

Monday 31 March 2014

Ordered by the House of Commons to be published on 31 March 2014.

Written evidence from witnesses:

- [Callcredit Information Group](#)
- [CIFAS](#)
- [Nuance Communications](#)

[Watch the meeting](#)

Members present: Dame Anne Begg (Chair), Debbie Abrahams, Graham Evans, Sheila Gilmore, Kwasi Kwarteng, Nigel Mills, Dame Angela Watkinson

Questions 82-154

Witnesses: **Jan Smith**, External Affairs Director, Callcredit Information Group, **Simon Dukes**, Chief Executive, CIFAS, and **Sean Duffield**, Partner and Public Sector Director, Nuance Communications gave evidence.

Q82 Chair: Thank you for coming along this afternoon. This is the second of three evidence sessions in our very short inquiry into fraud and error in the benefits system. I appreciate you giving up your time this afternoon to help us understand how it is dealt with in the private sector and whether there are lessons for the public sector with regard to what is happening. I wonder if you could perhaps introduce yourselves for the record, starting with yourself, Simon.

Simon Dukes: Thank you. I am Simon Dukes. I am Chief Executive of the fraud prevention service, CIFAS.

Jan Smith: I am Jan Smith. I am External Affairs Director at Callcredit Information Group.

Sean Duffield: I am Sean Duffield from Nuance Communications. I look after our partners and the public sector in the UK.

Q83 Chair: Thanks very much, as I said. Can I just start with an easy one? The Department for Work and Pensions reports its estimates of fraud and error in the benefits

system together. Is there a case for separating these two things out, because they are after all quite different?

Simon Dukes: Certainly from my view, yes, there is. I know that Cabinet Office figures talk about 80% of fraud and error within Government being down to HMRC and DWP together. It is important to identify these two together and to split them apart to identify how much is fraud and how much is error. Only by doing that and measuring it can we actually measure success against it, so, from our perspective, yes, it would be useful to do that.

Jan Smith: I agree with Simon. I think they would be far easier to understand if they were separated, because you are dealing with two completely separate things. On the fraud side, it is more about detection and prevention; on the error side, it is more about recovery of funds that have been done either through consumers' error or through Government error.

Sean Duffield: I agree with that statement.

Q84 Debbie Abrahams: Visa Europe says that its approach to setting fraud benchmarks is based on establishing an overall "risk appetite". Do you support a risk-based approach to benchmarking?

Simon Dukes: If I may, there are two things there. You talk about risk; I would be interested in that. I am slightly more concerned about benchmarking. In my own organisation, we do benchmark, but only organisations against a sector rather than benchmarking against other organisations. We do that because we are a not-for-profit organisation and we feel that fraud prevention is not a competitive issue. There is a concern if you are benchmarking one organisation against another that there is some sort of competitive element in it, so I would be cautious about benchmarking against other organisations.

Chair: Could I ask you to speak up just a bit, please?

Simon Dukes: Sorry. As you can probably tell, I have a slight voice problem. I will try my best.

Chair: We might be asking a question on voice recognition.

Q85 Debbie Abrahams: Does anybody want to add to that?

Jan Smith: I agree with Simon that, with benchmarking, you have to be very cautious. A risk-based approach works well in the private sector; it could work well in the public sector. By taking that risk-based approach, you have more flexibility with your resource, because the low-risk cases can be dealt with by one area and the high-risk cases by investigators, etc. In terms of managing resource, it would be helpful.

Sean Duffield: It is interesting to look at what sort of transactions may generate the highest risk. You may want to use systems that identify if somebody wanted to know where their nearest job centre was. This is very low-risk; do you even need to know who that person is? If there is a large change of circumstances going on, you may want to then

up the profile and understand further details about that person, so you may want to profile like that. I cannot see that benchmarking against banks is going to bring a lot of benefit.

Q86 Debbie Abrahams: Moving on to thinking about the public sector as a whole, do you think that there is a place for benchmarking in the public sector? Thinking about, for example, our experience in Work and Pensions, do you think that there is an acceptable level of loss that we should be looking at in relation to fraud now?

Sean Duffield: We could all agree that some fraud and error has an inevitability about it, but are we even sure that the fraud and error have been identified? We have a situation where we look at these figures, but do we in depth know the fraud that is happening? Has that level of investigation even happened?

Q87 Debbie Abrahams: You are casting some doubt then on the figures we have or are currently working with at the moment. Is that what you are saying?

Sean Duffield: Obviously I can read what is in the public domain. This gives the levels of fraud and error, but the information that I do not have is how that fraud and error is happening. It is quite difficult to make that judgment.

Q88 Chair: There could be quite a large proportion of unreported fraud or they just never found it in the system. Presumably that is not necessarily the case with errors though; you would expect most error to eventually come to the fore, but fraud could be just so very clever that you do not know it is happening.

Sean Duffield: Yes, precisely. Fraud by its nature may not have been uncovered. Error by its nature does tend to come to light.

Q89 Debbie Abrahams: Thinking then again about Work and Pensions and the different types of benefits that are claimed, do you think that looking at specific social security areas would be a more appropriate way of being able to stratify that to understand more about what the figures are telling us?

Simon Dukes: Could I just come back on the acceptable level? We are talking about public money and I do not think there is an acceptable level. There is no acceptable level in the private sector. What do we want to do? We want to reduce fraud so that it is as low as possible. I do not think we can talk about acceptable levels.

Q90 Debbie Abrahams: What is as low as possible? You have hit it absolutely. I could not agree with you more; it is public money, so what is the lowest possible level, because that is still a level? What is it?

Simon Dukes: Every organisation will have its own risk appetite, but we facilitate sharing of confirmed fraud data between organisations so that they can triage, investigate and then calibrate resources accordingly to prevent fraud, ideally, in the first place, because prevention is better than cure. Then, what is left you investigate. It would be wrong to start saying, "This level of fraud is acceptable in some way", because I do not think it is.

Q91 Debbie Abrahams: I could not agree with you more, but you are also, by what you are saying, saying that zero is also something that is unachievable.

Simon Dukes: Pragmatism tells you it probably is, but it should not be.

Debbie Abrahams: That is the point.

Simon Dukes: It is still something that you should aim for.

Q92 Debbie Abrahams: Is one way to understand the figures more fully to have more scrutiny and look at fraud and error within different social security areas?

Sean Duffield: Again, there are going to be areas within social security where fraud is more likely. I am not an expert on the different types of benefit payment, but there are going to be some benefits and areas of benefit that are more susceptible to fraud than others.

Q93 Debbie Abrahams: The final question from me: the National Audit Office is exploring with DWP the possibility of benchmarking the Department's processes for scrutinising benefit claims "against comparable administrative processes with similar levels of complexity in the private and public sector". I am sorry that was such a mouthful, but I needed to get that quote out. What examples are there of comparable and similarly complex processes in the private sector?

Simon Dukes: What the private sector has been doing for 25 years, if not more, is sharing its confirmed fraud data between itself, and that has proved very successful in preventing fraud.

Debbie Abrahams: Okay, so data sharing is key.

Simon Dukes: It is a key issue.

Q94 Nigel Mills: Can I just go back to what level of fraud on the state you might loosely call "acceptable"? Clearly, you would not call anything acceptable, but presumably when DWP are trying to design systems to spot fraud or error, there must be a level at which that fraud or error needs to be before investigating if it is really cost-effective. Tesco does not prosecute everyone who nicks £1 out of the till but, presumably, if someone tried to hack into Tesco Bank and nick £1 million, they would take a lot more of an approach.

Jan Smith: That is down to the risk-based appetite, again, for fraud. You will have different measures within different local authorities to what they see is a case that we should put our main investigators on. We need to throw lots of resource at it. If it is a massive fraud, we need to make recovery. Quite rightly as you say, Tesco does not prosecute everyone, and there is a lesson to be learned from that. If there are some small lower-risk cases, at the end of the day, there is limited resource. It is public money, as Simon quite rightly said, and someone somewhere has to take a view of how much we actually spend to recover something that is not going to be of benefit.

Q95 Nigel Mills: This is particularly hard because, if I am entitled to £100 of benefit this month and next month I am entitled to £75 because my status changes and I forget to tell

you, is that a mistake or is it a fraud? I guess that depends what view you take. It is not an easy or binary position in this situation.

Jan Smith: It is not easy, but the experience we have had, particularly with some of the local authorities we have worked with on council tax discount, is that different local authorities have identified people who are no longer living alone by sharing data and they have then adopted different strategies to tell people. It could be a soft letter that says, “It appears you have had a change in circumstances. You have not communicated it to us. You are no longer eligible for the discount.” People just go straight away, “Sorry, my mistake. Didn’t realise; forgot to tell you. I didn’t know I needed to do it.” Others have been more hard-nosed about it and sent someone round to knock on the door and check if there is more than one person living there. Again, it is down to the risk appetite and the strategy of each individual authority. The difficulty for them is finding that information in the first place to then act on and put resource into.

Simon Dukes: There is something there about checking through the lifecycle of the claim, not just at the application stage—the initial stage—but throughout.

Q96 Dame Angela Watkinson: 42% of over-payments are due to incorrect information on earnings or income, so should real-time information on earnings reduce incorrect payments once tax credits are brought under universal credit?

Sean Duffield: The answer could be yes, as long as people are doing that real-time reporting. I would say that that then creates a situation where people may not do that, but there would be a £75 or £100 example, letting that run out of time. We need to be very careful with real-time reporting. There are lots of ways that people can report their income, whether that be over the internet or the phone. It needs to be made very easy for people to do this. Also, if you see somebody who is weekly reporting their income and then suddenly stops, it would seem reasonable to use systems to jog that person’s memory to ensure that income reporting is happening.

Q97 Dame Angela Watkinson: It is a question of verifying the information that is given, is it not, because accurate benefits depend upon accurate information in the first place and what level of effort can be put in to verifying the original information that is submitted?

Jan Smith: That is the point at which people are actually making a claim. The fields that they complete and the information they provide in that claim need to be standardised. Everybody needs to be filling in the exact same form, providing the exact same information, no free format. You have to have values in because, if you have the accurate data, it is far easier to follow up when someone’s circumstances change. In the private sector, there is technology available that allows monitoring to take place so that, when there is a change in someone’s circumstances, you can be proactive about it. If you do not have the correct information in the first place, it is difficult.

Q98 Dame Angela Watkinson: Would that system also highlight the small proportion of people who are repeat offenders?

Simon Dukes: Yes. Certainly in the private sector, in the world that we inhabit, I would say that 40% of what we call re-filings are fraud that is being put into the system, into our databases, as being conducted by fraudsters who are already there, who have conducted

fraud in the past, not necessarily against the same victim or indeed the same fraud, but the same fraudster. The element of recidivism is relatively high at 40%, I would say.

Q99 Chair: Is there anything in the private sector that is as complex as the social security system, both in terms of the volumes, the numbers going through it, and the incredible churn when you think of the hundreds of thousands of people who are reporting every week a change of circumstances or the quarter of million who are moving in and out of work, every month? That constant is not just one thing that is changing; it is two or three different elements that might be changing in that. Is there anything comparable in the private sector?

Jan Smith: In the private sector, the major banks have worked over the last few years very much on what they call a “single customer view”. If you think of a bank for example, it has various divisions. It has a credit card division and a loan division. Sometimes within the banks, the banks do not know what is happening in one division and another but, with that single customer view, they know exactly what is happening with that customer so, when there is a change in circumstance, everything is updated.

Q100 Chair: They are just moving money in and out. They are not doing the calculation and entitlement, because there is the entitlement, the calculation and then there is the payment. All those things might change a couple of times in the course of one month—from week to week, in fact.

Jan Smith: I totally agree with you on that but, if you know you have that customer and you know the different benefits they are entitled to and what is happening with them, if there is any change in circumstance, you are in a far stronger position to reduce any areas and stop any fraud that may take place.

Q101 Chair: Have you got any sense of whether that should be done as an individual or as a household? When we go to universal credit, the assessment will be on a household base, with one payment a household. We were hearing in the last evidence session that, at the moment, housing benefit fraud can be picked up by the local council because they hold the register for the property but, when it goes to universal credit, it will be the person. There could be two claims going in for the same household and they do not have the data, unless they do the data-exchanging. Have you got any sense of how much more complicated it is likely to be if it is household income that is going to be managed through the social security system?

Jan Smith: It would be more complex to do household than it would for an individual. I do not have anything to back that up, I am afraid.

Simon Dukes: On complexity, we are just talking about data and there are some very complex systems in the private sector, but it is just data. Now in the 21st century, we can handle that quite easily.

Chair: It is just stuff?

Simon Dukes: It is pipe work; it is plumbing. I am not sure that the complexity of it should concern us too much.

Q102 Nigel Mills: Might it be helpful if I just gave you two scenarios and you told us what sort of thing could be done to try to tackle each fraud? The first scenario is an organised crime fraud, where you are getting people who do not exist to make a claim or perhaps people to make a claim and the money just goes straight through them to the people behind them. The second is the situation where someone is entitled, but the amount you are paying is clearly wrong. They have perhaps got some other income. How can you spot that before two years have gone by and there is a huge amount owed? Are there things out there that could tackle either of those two scenarios?

Sean Duffield: For the first scenario that you outline, for instance, I have a technology of voiceprint identification so, if somebody was contacting on one channel and then being somebody else on another channel, I could potentially, with other pieces of data, identify that you have that duplicate fraud happening there. It becomes a lot more difficult if an individual is just over-claiming; that they are under-reporting cash payments to them. It is hard to crack that small casual fraud, if you could categorise it as that, versus a fraud that is more organised and systemic.

Jan Smith: The fraud hub that we have set up recently is working around London and other regions, because fraudsters tend to move within regions rather than nationally. We have had some successes on the housing benefit side, where we have identified people for the local authority who have moved from one area to another, who were known to be claiming housing benefit in two or three different local authorities. That is fraudulent claiming of housing benefit. If you are looking at individuals and looking at boroughs, it is easier than serious organised crime, which is far more complex.

Simon Dukes: The frauds that we see, from the more than 300 organisations that participate in CIFAS, are across-sector. A fraudster does not just look at defrauding the banking sector or the mobile telecommunications sector; they go across. Data sharing between and within those different sectors often highlights precisely both the issues that you have talked about. I would say that confirmed fraud data sharing would highlight both of those, even the opportunist, because the chances are that it is not just that particular type of fraud that that individual might be committing.

Q103 Debbie Abrahams: Can I ask Jan about what she said just now: that fraud tends to circulate in regions rather than nationally? We could all have our guesses as to why that is, but what is the evidence about why that happens on a regional basis?

Jan Smith: What we have found with the local authorities that we have worked with is that people move from one borough to another, and they keep moving around and keep moving around. What actually keeps them in that region I honestly could not say. We could do some digging and perhaps provide additional information later, but it may be just something as simple as they have family in that area.

Debbie Abrahams: It is the same people?

Jan Smith: Yes.

Simon Dukes: We see a similar thing. We have washed our data against Ordnance Survey to look at heat maps and trends, and we have found exactly the same thing: that often, although not always, there will be a particular geographic accumulation of a particular

type of fraud. That might be because of the data that has been bought and sold by the fraudster in order to conduct fraud in that certain area. It could be because there is some criminal activity in that area connected with the type of fraud being conducted, so there are geographical hotspots, most certainly.

Chair: Perhaps we could ask where they are. We now have some questions on the investigation and prosecution of fraud cases, and Kwasi has the questions.

Q104 Kwasi Kwarteng: I just wanted to ask about the private sector. The private sector would typically take a view looking at the monetary value of the fraud and investigate whether it is worth their while to actually look at the fraud. What is the position in the public sector, do you think, with regard to the investigation of fraud?

Jan Smith: When we started working with local authorities to pull this fraud hub together and produce a fraud product, a lot of the benefits they were looking for from it was making it a swifter process to identify fraud in order to manage their resources more effectively. The way that we deliver information can be used by anyone, so you could have someone frontline who identifies, because of all the data that is washing around, that this is a potential fraud case. We identify them as red, amber or green so, if you get a red case, that probably means it needs to have full investigation; you need to do your Section 29s. That is going to be resource-intensive. Some of the lesser frauds can be dealt with by other people, so it helps local authorities manage their budgets more effectively.

Q105 Chair: Could you explain what Section 29 is?

Jan Smith: In the public sector, if you identify what you think is fraud, you can, under Section 29 exemption, come to a credit reference agency and access a lot more data than you would be able to normally to investigate that fraud. They are used by public sector investigators, but you have to be fairly confident that there is a serious fraud taking place. You cannot just do a blanket case for everyone.

Q106 Kwasi Kwarteng: With respect to prosecution rates, would you like to talk more about the rates at which only 28%, as I understand, of the cases that you have investigated in which a recoverable benefit was identified resulted in a prosecution? Would you like to comment on that? Do you think that is a good rate or something you might improve? Given the circumstances, is that realistic, and you could not do any more to prosecute those cases?

Jan Smith: I would not like to comment, because we provide the data; the local authority actually takes the prosecution.

Simon Dukes: Clearly, it is quite low, it seems to me. I am sorry to sound like a stuck record, but I think that, when you are looking at identification and investigation of fraud, accumulating evidence and then trying to recover the moneys that have been defrauded, it is an enormously resource-intensive process for the agency concerned, not only getting the money back but then covering the cost of all that activity. For me, I think we need to look at prevention at the start of the process, rather than looking necessarily—you have to do both, but prevention would help reduce risk in the first place. It would mean that, if it continues, if it is static, 28% might not be quite such a concerning figure.

Kwasi Kwarteng: The idea is that you would reduce the numbers at the beginning, if you like, and then, if you keep the numbers of prosecutions, that would be a higher proportion?

Simon Dukes: Exactly.

Q107 Graham Evans: The Government has talked about digital by default, for example for jobseekers in Jobcentre Plus. If you are going to be working in the 21st century, the idea is that some way or other you are going to have a computer. That is a mantra. Technology, I am sure we all agree, can help with identifying fraud. A question for you, if I may, Sean: IDA, the identity assurance for universal credit, is apparently some way off. I understand that it is “overly complex and potentially unwieldy”. Can you expand on that view?

Sean Duffield: I am not sure of the detail, because not a lot has gone into the public domain yet, as I understand, for that process, especially when it comes to how that is going to work on the telephony channel. You mentioned at the top of your question digital by default, and I would just caution on that. Today, we know that 11% of the population have got very low skills when it comes to using the web, so we need to make sure that, if people want to identify and verify with the DWP, they can do that across channels, both web and the telephony channel. We need to make sure that we have processes for security across all those channels that are also the same across those channels, so you do not need to know one set of passwords for the web channel, for instance, and another set for, let’s say, the telephony channel. From what I know about IDA, we need to make sure that it works across all the channels. At the moment, I have not seen any information on how it will work on that telephony channel and only some ideas about how it would work on the web channel.

Q108 Graham Evans: Howard Shiplee, the DWP senior responsible officer for universal credit, told us in February that “no one is using a totally online approach”. Do you agree that an entirely digital approach to this thing is feasible, achievable or indeed desirable when dealing with financial transactions?

Sean Duffield: I do not think it is a good idea, no. Nobody in the commercial world has really achieved that and people who have set out to just have a web service, quite commonly, have then ended up with call centres. We need to have inclusive services across all the channels. To become too dogmatic—that you will use the web—is not really the way forward, when we know that 11% of the population have not got the skills to do that.

Q109 Graham Evans: Out of the 11% of the population, what sort of demographic are they? Are they people over the age of 50 or 55 who did not experience IT at school? As the demographic changes and they are claiming benefits, they would have at least been exposed to some. What sort of demographic is that 11%?

Sean Duffield: It is weighted towards the elderly. It is weighted towards people in lower socioeconomic groups. We could say that the disadvantaged in society probably take the main brunt of that 11%. When we see things like income reporting coming up and being

central to the way benefits are going to be paid in the future, it will be really important that we have channels that are open to everybody.

Q110 Graham Evans: What would you say is a private sector solution to that problem?

Sean Duffield: They give people choice and they make sure that those choices are appropriate. For instance, I can phone my bank, I can get my balance and I can make payments that way, or I can go on to the website and do that.

Graham Evans: That is by picking up the telephone and speaking to somebody?

Sean Duffield: Or it is an automated system. What we would say from Nuance is that, if you can deal with things in automation, do them in automation, especially on the telephony channel, because you have a very valuable resource there of people. If those people are doing higher-value things—they are advising people around their entitlements, making sure that people get what they should be getting—that is an awful lot better than people giving low-value information out, for instance doing identification and verification, telling people where the local job centre is and all those things, which could easily be done within automation.

Q111 Graham Evans: I am afraid there is another question for you, Sean. There was a very interesting exercise in Australia with voice verification identification to avoid fraud. Can you give us some more information on the background to that?

Sean Duffield: Yes. This is Centrelink, which is the department of social security in Australia. They are running an income-reporting line. What they were finding was that they gave people passwords, but people were forgetting those passwords. That was then stopping income reporting, so they have built a system now that is automated. You go into that and just using your voiceprint, based on previous calls, you just need to know your account number in fact and then, through your voiceprint, the rest of the identification process is done. It has saved a lot of time and increased reporting.

Q112 Graham Evans: The question is: can it be easily impersonated?

Sean Duffield: No. It is very hard to impersonate. Like all technologies, it is not 100% but, when you combine it with knowledge-based information, i.e. your account number and the voiceprint, it is a very secure way of transacting. No, I could not do an impersonation of you to get into your account.

Q113 Graham Evans: Or Rory Bremner would not be able to?

Sean Duffield: Rory Bremner would fail badly. It is looking at around 100 data points. We use a number of those. It is looking at vocal-tract length and the pitch that you speak at; it is taking lots and lots of factors of the voice.

Q114 Graham Evans: If you have an illness, a sore throat or whatever—

Sean Duffield: There is a point where, if your own mother would not understand you—as with all technology, there is a limit.

Q115 Graham Evans: It sounds very interesting. I believe it started in 2009. Do you know, as of 2014, how successful it was in reducing the level of fraud?

Sean Duffield: I have read a report and I have it here. They say that there has been no fraud that has happened through that line, using the voiceprint, but I need to confirm that.

Q116 Chair: I suppose we will need to know what kind of fraud was possible before that is not possible now. I presume that there was some fraud, but somewhere else in the system.

Sean Duffield: Precisely, and the use case for that, yes, was to look at fraud, but it was also for convenience because so much time was being wasted doing password resets.

Q117 Graham Evans: Do you have any figures that you could share with the Committee?

Sean Duffield: I will dig out and share what I can.

Q118 Sheila Gilmore: Sorry to have come in late; I had another meeting to go to. Are there any large-scale users of a system like this here in the UK?

Sean Duffield: Barclays Wealth has deployed a biometric solution.

Sheila Gilmore: Is that a voice solution?

Sean Duffield: Yes. You phone into Barclays Wealth. The first time you phone in, it will put you through the standard identification and verification process, asking you the third and fifth letters of your password, as you would with your bank normally. Once they have then captured your voiceprint, you are offered an enrolment, "Would you like to enrol in the process?" Most people say yes; 93%, I believe it is, say yes. Subsequently, when you phone back into the bank, you just give your account number and then, through talking to the agent for around 15 seconds of audio, that is sufficient for them to let you in to use your banking services.

Q119 Sheila Gilmore: What sort of numbers are involved?

Sean Duffield: I do not know the numbers for Barclays, but I know that in Turkey Vodafone are into the millions. I would need to check those numbers and I will let you know, but they have millions of enrolments into a biometrics process there.

Q120 Sheila Gilmore: The issue, particularly around the discussion on universal credit identity, has been that this is not just a question of letting people supply information, but it is also giving people things. Is what is happening in Australia tied into people's payments that they give?

Sean Duffield: Yes. It is done on an income-reporting line. Just as under universal credit where people are going to have to report their income, that line was set up so that people could report their income. Obviously it cuts both ways. You do not want people falsely reporting income to people or being malicious as well, and it prevents that.

Q121 Sheila Gilmore: Do you mean another person?

Sean Duffield: Yes. The use case for this technology is it stops imposter fraud. You can also start comparing voiceprints coming into an organisation to make sure people are not taking out duplicate enrolments.

Q122 Sheila Gilmore: Given that we have been talking about identity stuff in terms of universal credit, almost from the day it was first mentioned, I am quite surprised that this has not been mentioned to us before as a possibility, because it has been one of the real problems in getting a working IT system. We were told that one of the reasons for the slowing up and so on was that this was one issue that had not been properly resolved. Is this quite new as a technology?

Sean Duffield: The technology has been around a while now. There are a number of deployments out there. As more organisations take it on, more organisations will go with it. There has been that slight element that it is new, so people have been a little wary of deployment. However, I want to emphasise that this voiceprint technology is part of this overall solution. If I do not have correct data in the first place to enrol people, I may enrol fraudsters. I need to have data based on credit histories and all of these things, so I know that I am not enrolling fraudsters in the first place. It is not the be-all and end-all; it is part of an overall solution.

Q123 Sheila Gilmore: It would really be after the first bit. You described it as working in a system that is already up and running, and people are simply giving more information.

Sean Duffield: There are two types of system that you can deploy with speech-print technology. The first is called text-independent, and that is what Barclays has deployed. When you phone them, you give your standard identification and verification tokens, and then you are enrolled in the system.

The other way to roll people into a system is that you can do it automatically by, for instance, sending them out a letter, asking them to phone a number, giving them a one-time token to use a number. They then phone in and say, "At the DWP, my voice is my password". They say that three times. We then have that voiceprint. Next time they phone in they could give just their National Insurance number. They could then say, "At the Department for Work and Pensions, my voice is my password", and they would then be into the system. There are two ways you can do it: you can do it with an agent-assisted way using the say-anything technology, or you can use text-dependent technology where people have a set passphrase.

Q124 Sheila Gilmore: How does that fit with online then?

Sean Duffield: Online, with identification and verification, there are three elements. There is information that I could write down, so my bank account number, my date of birth, or my mother's maiden name. That is information that I could give to somebody. The other information is something about me: my fingerprint, my voice, or my iris. The final bit of information is maybe something that I have: a mobile phone. If you did three-factor authentication of people that is very, very hard to sidestep, whereas

knowledge-based identification and verification can be sidestepped, because somebody can simply just write that down and give it to another individual. For instance, on the web channel, let us say I have filled in a web form and what I was doing had the potential for fraud, a telephone call could be launched out to my mobile phone that I could then verify my voice on that it was me sitting in front of that web form. You can start to use these technologies across channel to secure identification and verification. As we have touched on earlier, if we can secure an organisation, it is a lot better to secure it before any fraud has happened than go and try to find the fraud subsequent to the event.

Q125 Chair: Can I ask what the other two think of this?

Simon Dukes: All I was going to say is it is an ID assurance process; it is not a fraud-prevention process. Fraud prevention is a very clear by-product from this but, as Sean said, you have to have ID assurance alongside fraud prevention as well. You have build fraud prevention into your system.

Jan Smith: I agree totally on that.

Q126 Chair: This is totally different from the software that picks up if somebody is lying, which in some areas has been discredited but is still being used by insurance companies and things, I think?

Sean Duffield: It is nothing to do with that.

Q127 Dame Angela Watkinson: I was wondering about social networking in that it is notoriously insecure. To what extent, if any, do you think that it could be used to compromise online identity verification and identity theft, for example? Has it a role to play, do you think?

Simon Dukes: Very much so. Of the frauds that we see, the external consumer frauds that are being conducted, either because people are using false identities or stealing somebody else's identity, in that latter part, 60% of that makes up the frauds that we see. Of that, 80% is committed online. The type of harvesting of data and information online is of great use to a fraudster, whether it is from their social networking site, whether it is from public accountable records, Companies-House-type records, where you have the details of people's name, address and date of birth, all that sort of data can help a fraudster steal and take your identity.

Jan Smith: It is not just necessarily online. I do not think people realise how sensitive their personal data is and how easy it is for other people to get hold of it. I travel frequently on the train down to London and I hear people on their mobile phones on the train. They are giving out their name, their date of birth, their credit card number and their address. Anyone sat within a 10-foot radius can capture all that information and then steal that person's identity. I suppose this is a bit cynical of me, but, if you were a burglar sat on that train, you would know then that they are going to be out of the house between 9am and 3pm, because they said not to deliver then. It is no wonder criminal gangs are all working in cohorts with each other. People giving out sensitive information is not necessarily just online and not necessarily just social media.

Chair: I hope nobody was in the BA lounge this morning when I was just doing exactly that.

Q128 Dame Angela Watkinson: Could I start by asking Jan Smith to say a bit more about the ThreeSixty Hub, which is a data-sharing process between London local authorities? I know it was quite difficult to get it started and get the permission to go ahead. I wonder how it is working. How many London local authorities are now participating and are others showing an interest so that it might grow?

Jan Smith: We are still having some difficulties with people agreeing to share data with us, but that is more of a data protection and legal problem than an intention of local authorities to participate. Basically, the ThreeSixty allows a number of boroughs—and I will have to confirm the exact number later—that agree to share with each other the data they are allowed to share, for example tenancy data or tenancy waiting lists. Some share housing benefit—others do not—and council tax reduction data.

There are two ways then that the local authority can use the data that is in that hub. They can either do what we all a batch process, which means they say to us, “Here is everyone we have on our books. Run it past what is in the system and, if you identify anything that you think may be fraud, we can then go away and investigate it.” Others use it at point of application. If I, for example, went down the road to the local authority and said, “I’m Jan Smith. I want to claim housing benefit. I want to go on your tenancy list,” they could then look and make sure that I was not already residing in another borough and claiming housing benefit in that borough. There are two points for it: there is the application stage, and we talked about customer management before, where occasionally you will run everything through the system to make sure that there are no frauds popping up that you were not aware of at application point.

Q129 Dame Angela Watkinson: Do you foresee that it is going to be a useful thing once it gathers momentum and more local authorities take part?

Jan Smith: Yes. The feedback that we have had from the people who are using it—one borough has just started using it at application point and they are identifying over 10% of potential fraud cases at application point, each week. Some of the others that have used it have given us case studies that I can provide to you.

Dame Angela Watkinson: I would be interested in that.

Jan Smith: They have identified elements of fraud and what it has cost them to try to recover that fraud against the income losses. There are case studies out there. The difficulty that we have had with it, which is again about data sharing, is people’s understanding of what data they can and cannot share between themselves. There is no clear guidance coming from anywhere. Each local authority’s legal department takes a different view. For example, we have had people saying, “We cannot share housing benefit with you. We are not allowed to do that,” yet the Serious Crime Act of 2007 says that public sector data can be shared with the private sector where it is to be used for prevention or investigation of fraud. Whether people are hiding behind those excuses because they do not actually want to do it, I am not sure, but there is no clear guidance that says, “Here’s what you can share; here’s what you cannot share.” In the private sector

there is; there are rules on reciprocity and there are rules on data sharing. That has been a stumbling block for us.

Q130 Dame Angela Watkinson: There is a need for clarification and proper guidance for local authorities?

Jan Smith: Yes. We had a case with two authorities where we talked to the ICO and got guidance on data protection; that was fine. We got a legal view; that was fine. Just to be certain that they were not doing anything wrong, the authorities went to DWP, which told them something completely different. On the basis that they did not want to incur any ICO penalties or anything else, they decided not to proceed.

Dame Angela Watkinson: They erred on the side of caution?

Jan Smith: Yes.

Q131 Dame Angela Watkinson: There is a need for accurate, consistent advice?

Jan Smith: Absolutely.

Simon Dukes: And not just local authorities, but with DWP, HMRC and other large Government agencies.

Q132 Dame Angela Watkinson: Could I just move on to private sector concerns? A number of witnesses in previous meetings have told us that DWP could prevent and detect a significant proportion of benefit fraud and error if it had greater access to or made better use of private sector data, such as credit references and banking and payments information. Do private sector organisations have reservations about making this information available, for example, due to the risk of reputational damage in the event of a breach of data protection law? That really comes back to the previous comment about knowing exactly what you are allowed to do.

Jan Smith: We talked earlier about the Section 29 exemptions to the Data Protection Act. If an investigator in a local authority exercises that Section 29 exemption, they have access to people's financial and credit data, and all the information that would be available in the private sector, so that can be done.

Simon Dukes: As I said earlier, it is this idea of preventing fraud and not seeing it as a competitive issue. In the private sector, what we have within CIFAS is over 300 organisations doing precisely that—exchanging and sharing their confirmed fraud data with each other, on the understanding that they will get value from doing precisely that. In the last 12 months, we saved those organisations £1 billion of fraud loss. We believe you extrapolate that to the public sector as well and get similar benefit from public/private sector sharing.

Q133 Dame Angela Watkinson: Would you say that there are opportunities for the private and the public sector to work collaboratively or co-operatively together in combating fraud, to the benefit of both sectors?

Simon Dukes: Absolutely. I find it extraordinary that we do not. Fraudsters are quite keen to exchange information between each other, and buy and sell data on individuals' identities and collaborate. I find it extraordinary that we in the UK do not have a similar type of attitude to data sharing in order to defeat fraud.

Dame Angela Watkinson: That is very helpful. Thank you.

Q134 Nigel Mills: I can see the argument for having that kind of data sharing to combat fraud. I guess where we start to get into issues is how much data sharing you can do just to check that my claim is right and I do not have some other income, and have perhaps not earned £50 more this month than I am saying. Does that give you the right to check my bank account? Where do you reckon the right balance is on this situation?

Simon Dukes: We are only looking at confirmed fraud data, because of the 40% recidivism that we talked about earlier. Checking at the point of application, checking throughout the process of the claim or through the client's journey with a particular organisation, will help you identify if there are frauds cropping up, as has already been mentioned. Looking at it purely from that fraud perspective, if you have a threshold for reporting that type of fraud, then somebody who has inadvertently done what you suggested would not hit that threshold and, therefore, would not be logged and would not be fined.

Jan Smith: Some of the law is there already around data protection. The first data protection principle says that processing of personal data should be lawful, so I think some of the protections that you may be concerned about are already in place. They are just generally misunderstood and not interpreted correctly, so they are not used effectively and properly.

Q135 Nigel Mills: Say you wanted to look at bank data and say to the banks, "Here is our list of people we are paying large amounts of out-of-work benefits to. Can you just cross-reference your data and just see whether anything flags up, like a large monthly salary turning up that might look in conflict with what we are doing?" that is a bit different from there being a fraud we can reasonably suspect on a case-by-case basis, to a more proactive, "Let us look through a whole list of data to see if we can spot a problem starting". What is your analysis of the data protection implications of doing that? Could the banks actually comply with that?

Jan Smith: It is a difficult one, because consumers quite rightly are very protective of their data. There are ways and means of doing things with their consent, and data-sharing guidelines that mean it could be done. It would be difficult to come to something that kept everyone happy, because even when there is legitimate reason for processing personal data, consumers are still very uptight about it and do not like it. It could be explored in more detail. The bit Simon's talking about, where you know it is the confirmed fraudster, that piece is quite easy.

Simon Dukes: It is easy, but it has not been done. Let us start with that and then see where you get.

Q136 Nigel Mills: Ms Smith, in your written submission, you quoted the Information Commissioner who said something like "responsible data sharing in a good cause is always

possible”. Is what you are saying that it might be possible for the Department perhaps to be a little less conservative in its approach and try to push the boundaries?

Jan Smith: Exactly. A lot of it is about being able to do it and use the data but, on the other side, you have the consumer where there is an education process. This is my personal opinion now, I hasten to add. I am sure there are a lot of people out there who would not mind their personal data being used in that way, if it was going to stop their identity being stolen and if it was going to stop further fraud happening.

Q137 Nigel Mills: In theory, it could be a condition of claiming a benefit that you let us have access to all your data, anywhere we choose to go and find it. That might be going a little bit far.

Jan Smith: It could be a step too far.

Q138 Nigel Mills: Do you have any experience of HMRC being a little more proactive at using private sector data than the Department? Is that something that you perhaps have not seen any evidence of either way?

Jan Smith: We have done some work with HMRC, but more around the recovery side than fraud prevention. In the case of where errors have been made and recovery is required, we have done some work using data with HMRC on that, but nothing from the fraud perspective.

Q139 Nigel Mills: Do you think there are any further powers the Government needs to take, perhaps changing legislation or something? We saw some changes in the Prevention of Social Housing Fraud Act 2013, which allowed local authorities to ask for a range of information. Do you actually think more powers are needed or is it better use of powers that already exist?

Jan Smith: I think better use of powers that already exist and the removal of this confusion of what can and cannot be done, so you have a consistent approach, whether it is central Government or local government.

Simon Dukes: The Serious Crime Act 2007 quite clearly set up this SAFO type of organisation—a specified anti-fraud organisation—for the purpose of being able to facilitate public and private data sharing. It has not happened. Clarification of SAFO and what is written in the Serious Crime Act would go a long way to helping perhaps remove the logjam, and then there is a bigger cultural thing in some Departments about data sharing with the private sector. That is a different issue, but some clarification on the Serious Crime Act would go a long way.

Q140 Sheila Gilmore: There seems to be an assumption here, or maybe not, that the private sector data is accurate and, therefore, all we need to do is get it and it will all be fine. I have certainly had experience of difficulties that arise when people receive demand letters for debts that they do not owe; they may relate to somebody who used to live in the place. We have a lot of problems with our tenemental buildings in terms of what the address identifier is, which varies between different organisations. When they were doing the data matching for individual voter registration, there were large discrepancies between the information the electoral registration officer kept, in terms of addresses and so on. It is partly

about the way the addresses are. It is okay if you are just 16 Larch Avenue or whatever but, in my city and my constituency, a lot of the tenemental flats have differential numbering. They are not always using the same numbering, for all sorts of reasons. The Post Office decided to change them all at one point and change them in some rather peculiar ways.

Actually, people find that they are getting letters for other folk. It still surely needs a bit of common sense and fairness because, if it is done automatically, in this situation somebody could have their benefits stopped. I know people who have had their tax credits stopped on the basis of a data-matching exercise that was carried out by HMRC using credit rating agencies or whoever they are, and it was just not right. It was not right and their money has suddenly stopped.

Simon Dukes: We are talking about the differences between the challenges facing DWP and the challenges facing the private sector. You are absolutely right that DWP is going to have to pay claimants regardless of whether they have committed fraud in the past, if they are entitled to those payments. There is a different calibration here. What we are talking about is the benefits of data matching through data sharing to help calibrate risk. It is not an automatic rejection of anything and it should not be. Certainly the good practice that I hope that the organisations that work with us follow is that, if you have a data match, it is something that is then flagged up for investigation. It does not mean it is an automatic rejection of financial services or an automatic rejection of some sort of application for something. It is something that needs to be looked at more carefully, investigated, to see whether indeed that data match is worthy of saying, “Yes, we are not going to do that”. It is a risk calibration; it is a triage process.

Jan Smith: All the data matching we will do will raise exceptions. It is those exceptions that need investigating. The majority of data that is held by credit reference agencies is accurate. Nothing is ever 100%, but to take a policy, for example—you have just explained that you could not match this person at this address so you just stop making their benefit payments to them—it should be treated as an exception. You should do more investigation. That is what I was talking about earlier. You have your investigation officers who could actually go round to that property and make sure that person is still living there. The other 99% of cases that all match effectively are much lower risk; you can just carry on as normal with them. Data matching should highlight exceptions and the exceptions should be investigated, not just a clear-cut, “We’ll stop their benefits. We’ll stop making payments. We’ll stop delivering anything there.”

Chair: That leads us neatly on to confirmed fraud databases and Dame Angela again.

Q141 Dame Angela Watkinson: I have some questions for Simon Dukes. I am going to start by quoting you—I hope I am right—saying, “The current system for tackling housing benefit fraud is an example of perverse incentives driving poor outcomes, both in terms of fraud prevention and achieving law enforcement outcomes.” That leads to the question: do you therefore believe that the move from the current system to universal credit will drive out these perverse incentives and so better enable the Department to combat fraud?

Simon Dukes: Moving to universal credit should be applauded, absolutely, and I think it will have some benefits in reducing fraud risk.

Q142 Sheila Gilmore: How?

Simon Dukes: By the fact that we are going to an online system whereby, with assurance of identity, you will be able to—

Sheila Gilmore: The assurance of identity is the crucial bit.

Simon Dukes: It helps.

Sheila Gilmore: It is not actually universal credit; it is the assurance of identity.

Simon Dukes: What I was coming on to say, yes, as I have said—

Sheila Gilmore: Which has not been built into the system yet.

Simon Dukes: Fraud prevention is a by-product of identity assurance, as we talked about earlier. What I wanted to say was that my concern about universal credit is that, without a fraud prevention system built into it, the problem that you face is moving from your existing client book, the existing system, to a universal credit system and transferring, without trying to filter out the fraudsters, without trying to filter out the false identities. You are just putting on to a universal credit system the problems that you already have with the existing system. That is my concern and that is why I mentioned it in the letter.

Q143 Dame Angela Watkinson: Is there any evidence that demonstrates how likely it is that a person who has already committed one type of fraud is likely to commit another one?

Simon Dukes: As we have mentioned, the recidivism rate for fraud is high, but I would also say that this is about cross-sector matching. What the member organisations who work with CIFAS tell us is that 40% of the benefit that they get from data matching comes from data outside their own sector, because fraudsters do not just work against the banking system, the insurance system, or the telephone or retail system; they work across all of them.

Q144 Dame Angela Watkinson: Which public sector organisations are members of CIFAS?

Simon Dukes: It is a small but growing band of organisations. We currently have the Student Loans Company. We have Big Lottery. We have the Land Registry. The Charity Commission will be joining very soon, and we have Home Office immigration as well. The point is why they have joined rather than the fact that they are joining. The reason they have joined is that they are public sector organisations and they have seen the benefit of data sharing with private sector organisations.

Q145 Dame Angela Watkinson: Has there been an evaluation yet of the impacts of accessing CIFAS's data on rates in public sector fraud?

Simon Dukes: We provide sectoral-based assessments for our members. I do not have that data with me but, overall, our fraud loss for the last 12 months is £1 billion. Obviously a small proportion of that will be public sector, but they report to us the benefits of what they see in data sharing with us.

Q146 Dame Angela Watkinson: Do you offer data matching as well as data sharing?

Simon Dukes: Data matching, as we discussed earlier, is really what I see as the benefit of data sharing. You cannot data match without sharing data in the first place. Data matching is the value that you get from sharing fraud data amongst a number of organisations.

Q147 Dame Angela Watkinson: Have you discussed with the DWP the possibility of them joining CIFAS?

Simon Dukes: I would love the DWP to join CIFAS. I think there is a huge benefit for them in doing so. I have written to Lord Freud; I wrote to him back in October last year, precisely flagging up the issue about the universal credit move from the existing client book to the new system.

Q148 Sheila Gilmore: How much does it cost?

Simon Dukes: I said in the letter to Lord Freud that, because we are a not-for-profit organisation, it would be something that we could do pro bono to wash the data from your existing client book through to universal credit to remove and filter out the fraudsters, filter out the false IDs. He wrote back saying that that was not something that he would be interested in.

Chair: We can ask him next week.

Sheila Gilmore: You will do that work for nothing?

Simon Dukes: Yes.

Q149 Sheila Gilmore: What are you expecting DWP to do, because we are still dealing with real people who have an outstanding benefit claim? You are not suggesting some sort of automatic system that then says, “Right, that’s it; you’re off our books.”

Simon Dukes: No. What we have said is that none of this is an automatic rejection. This is allowing you to triage and identify where your risks are. Once you have identified where your risks are, you can allocate resources appropriately. That is what the private sector does. We are absolutely not advocating automatic rejection. That is not what we do at all.

Q150 Chair: You are really saying you are just flagging up, “There may be a problem here”. Extra investigation will be required in each case?

Simon Dukes: Absolutely, because we know how resource-intensive investigation is and how difficult it is, so at least point it in the direction of the greatest potential benefit.

Q151 Chair: This is possibly our last question, but the Committee often comes back when it thinks of other things. The DWP says it is developing, and I will read the quote, an “automated risk assessment service that will determine the likelihood of fraud in every new claim or change being processed”. Is it currently possible for this service to be automated?

Simon Dukes: I have not seen anything to suggest that it is in the process of being constructed. All I would say is that that system already exists. Therefore, why build something that already exists? I do not know; without having seen what this might actually consist of, it is very difficult for us to say any more.

Q152 Chair: My second question is: will the DWP have access to sufficient sources of data to enable it to assess claims and changes to claims? In other words, can they automate the whole system? We have talked a lot about the fact that they do not have access to a lot of the data that is held elsewhere and, without that access, can they therefore make the claim that they are going to automate the likelihood of fraud?

Simon Dukes: I would say that they need to start sharing data first, before they would be able to do that.

Chair: It comes back to that. You are agreeing. I am finished. Does anybody else have anything else?

Q153 Nigel Mills: I will ask the blue-sky question. If I put you in charge of this tomorrow, what would you change to tackle a) fraud and b) error? Is there anything that you would do that is not being done, which would make a real difference?

Sean Duffield: For me, I can provide systems that can look at data. I need good data to be able to drive automated systems to provide identification and verification services, and also to be able to drive anti-fraud. I would want to secure access to the Department. That is what the technology that I offer could bring. Once you have fraud within the system, it is hard to go find it, and then there is also that cost implication that we have discussed today: here is a fraud; is it now economic to actually go after that and prosecute that fraud? I would certainly be looking at very strong identification and verification processes based on good data to initially enrol people within these systems. That is the thing I would do tomorrow and across multiple channels as well.

Jan Smith: I would say pretty similarly that the data that is collected at the outset needs to be accurate and you need to have the ability to share that data to make sure you have identified the fraudsters, at that point of application. I think it can be delivered across lots of different channels. If you have people who can access the web, then they can serve themselves, but the data that is captured needs to be mandatory, so everyone is capturing the same information. For those who do not have web access, which we have talked about previously, have an assisted service where they can ring a helpline. Whether they do it online or over the phone, the same information is being captured and the same data is being shared to make sure that fraudsters are being identified.

Q154 Sheila Gilmore: Would there be an advantage in citizens having one identification system to deal with the public sector? We are dealing here with an awful lot about potential benefit fraud, but clearly there are other areas, such as how much tax people pay, that might be relevant. Should we not just have a unique identifier?

Sean Duffield: It would be a good idea. There are implications that flow out from that but, from a technical point of view, it is a really good idea. The politics of that idea to have one identifier on a national scheme is not for us, as the suppliers—

Chair: I thought it was called an identity card.

Jan Smith: You could say there is already a unique identifier in someone's National Insurance number, but we all know that fraudsters can quite easily get hold of National Insurance numbers and there are more National Insurance numbers in place than people who actually should have them.

Chair: That is right; there is a larger number than the population. Simon.

Simon Dukes: I worked in the public sector for 24 years, and I think there is a lot that the private sector can learn from the public sector. On fraud prevention, there is something that the public sector can learn from the private sector. It is a bottom-line issue for the private sector. They have evolved over the last 20 or 30 years in making sure that fraud prevention is part of their process. Data sharing works. It has worked for my organisation for the last 25 years. It absolutely works and you need to build it in, because prevention is better than cure every time.

Chair: I think we have exhausted our questions. I suspect we might have exhausted you as well. Thank you for coming along this afternoon. The evidence you have given will be very useful when we come to writing our report, so thank you again.

