HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Fraud, HC 125

Wednesday 13 March 2024

Ordered by the House of Commons to be published on 13 March 2024.

Watch the meeting

Members present: Dame Diana Johnson (Chair); Tim Loughton; Alison Thewliss.

Questions 398 - 521

Witnesses

I: Simon Fell MP, Prime Minister's Anti-Fraud Champion; Mark Cheeseman OBE, Chief Executive, Public Sector Fraud Authority; Nick Ephgrave QPM, Director, Serious Fraud Office.

II: Rt Hon Tom Tugendhat MBE VR MP, Minister for Security, Home Office; Baroness Vere of Norbiton, Parliamentary Secretary, HM Treasury; Duncan Tessier, Director for Economic Crime, Home Office; Anna Harvey, Deputy Director (Payments and Fintech), HM Treasury.

Written evidence from witnesses:

Public Sector Fraud Authority

Serious Fraud Office

Home Office

Examination of witnesses

Witnesses: Simon Fell MP, Mark Cheeseman and Nick Ephgrave.

Chair: Good morning and welcome to the Home Affairs Select Committee. I apologise for starting slightly late this morning.

We have two panels in our final session on fraud. The aims for this session are to examine the UK's response to fraud and the impact of serious fraud offences and fraud against the public sector; to understand what the Government are doing to combat the scale of fraud in the UK; and to examine the effectiveness of the Government's counter-fraud policies, including the fraud strategy and the economic crime plan. We are also very mindful that a fraud summit was held earlier this week, and we are looking forward to hearing about that.

Can I ask our witnesses this morning to introduce themselves?

Simon Fell: I am Simon Fell, the MP for Barrow and Furness. I am the Prime Minister's anti-fraud champion. For clarity and completeness, I should say that I am a member of this Committee and have recused myself from this inquiry.

Mark Cheeseman: My name is Mark Cheeseman. I am the chief executive of the Government's new Public Sector Fraud Authority, which works with Government Departments and public bodies to better understand and increase the impact of our action against fraud in the public sector.

Nick Ephgrave: Good morning, everyone. My name is Nick Ephgrave. I am director of the Serious Fraud Office, a national organisation that is designed to combat serious and complex fraud, bribery and corruption, usually international bribery and corruption.

Q398 **Chair:** Mr Fell, in your role as the anti-fraud champion for the Prime Minister, could you give the Committee a flavour of where you think we are now on fraud, and whether the Government are finally taking fraud seriously? There seems to have been a very long delay in getting a fraud strategy out. What is your take on that?

Simon Fell: When we are in a situation where we have such a prevalent crime as fraud—it is 38% of all crime at the moment—we are clearly not in the place we need to be. The fraud strategy is a recognition of that. We need to change the way we approach fraud, what we do to pursue fraudsters, the way we look after victims and the way we make the system work better together. Everything in that strategy is about delivering the sort of changes we need to make the system work better.

There is a huge amount of work coming out of that. I will rattle through the key points in it. You mentioned that we had an international summit yesterday; 70% of the fraud that we see in the UK has an international component. We are never going to be able to answer the question of how we deal with fraud if we just focus on the UK. We need to get data shared across countries. We need to get law enforcement working together so that we can better pursue the criminals who are causing these harms.

At the same time, we need to bring industry on board. Before I was an MP, I worked in fraud prevention. We would never have talked 10 years ago about bringing social media companies into the conversation. As we have heard in this Committee, a good amount of the fraud that is committed in the UK begins or is perpetrated across social media platforms. Getting them around the table, working with them, getting them sharing data, helping law enforcement, better protecting victims and allowing users to report fraud on their platforms are all key outcomes of the fraud strategy and are part of the online charter that we have managed to get over the line with a good number of these companies.

We are improving the victim response. We have the national fraud squad now. There are 400 officers in post, and there will be 500 by the end of 2025. All this is about changing the dynamic on fraud. Despite the fact that we have all this great work going on, if you look at each of these pockets in isolation, they will make a small difference to the bigger picture.

The learning is that there is no one silver bullet to this. It is about an entire system change, and the fraud strategy is a really good step towards that, but when we deliver all the actions in it, that is not job done. Fraudsters innovate; they look for holes in the system; they look to exploit wherever they possibly can, so we have to keep iterating and working together. It is about finding new partnerships, finding where the next vulnerabilities are, and then changing the system again and again and again.

Q399 **Chair:** Can you say something about data sharing? It is an issue that we have come across a lot in our inquiry. There is a lot of talk about how our institutions are good at data sharing, but are we really? Is there not a major problem with data sharing, particularly with the international issue that you have raised? So much fraud comes from overseas. Are we really good at getting that data sharing?

Simon Fell: You raise a really good point. In the UK, we have a number of really good data-sharing schemes up and running. I declare an interest: I used to work for one of them before I was in Parliament.

They collate data from across industry. They share it with law enforcement so it can be used in anger against criminals and so that victims can be better protected. That is now part of the infrastructure of policing and fraud prevention, and it is quite a successful industry as well. You can see absolute results from the sharing and use of that data, but you are right. The international component is key here, and it is also about learning where fraud is evolving and where it is moving to.

I mentioned tech firms in my previous answer. We need to learn from those companies what they are seeing. At each point in the fraud value chain, from an account being hijacked to a fraud either being enabled or taking place on a platform, to money leaving someone's account, what signals are going across that value chain? Where can that data most usefully be shared and in what format? We need to step up systems to make that happen.

That does not happen overnight. We have to be really careful when we enable these things, because there are concerns about data protection, people's privacy, and decisions being made about people's lives based on information across that piece. There is a huge amount of work in the fraud strategy and with law enforcement to get that right.

Then we start to look at the overseas component as well. As I said, 70% of fraud has an international component. When you see the moneys travelling overseas, we have to make sure that law enforcement has the legal ability to talk to its partner organisations in other countries, so that you can follow that money. You can go after the gangs.

Q400 **Chair:** In our very first session, on romance fraud, we heard evidence from a victim that she found it incredibly difficult, in terms of the international dimension in that case, to know what was happening and to feel that it was all being taken seriously by all the law enforcement agencies involved. It was not just one country; it was several. That evidence was quite powerful. Those links were not working in that particular case.

Simon Fell: Yes, and it is fair to say that we have a long way to go on this. The reason we have spent the last three days having a global summit on fraud was to talk to other nations who are experiencing exactly the same challenges at the same sort of scale, to get them into a place where they are prepared to work with us, share data and understand where data protection rules and disclosure rules get in the way of decent results in this space.

I was absolutely surprised by the co-operation that these countries offered. They are leaning into the same challenges. They recognise that we have a shared solution that we need to get to, so they want to work with us on it.

Q401 **Chair:** Did you get some hard outcomes from that summit? In the communiqué, there are lots of commitments. There are commitments to develop a better understanding of the fraud threat and to strengthen multilateral partnerships and grow capabilities; there are commitments to strengthen victim support and to support victims; there is a commitment to increase data intelligence sharing. That all sounds very positive, but are there hard outcomes from that summit that you know will be delivered by countries?

Simon Fell: They were good outcomes, because this is the first of its kind. We have never had a global fraud summit like this before. They came around the table. We brought some of the biggest tech companies in the world around that table as well. Law enforcement was around that table. We clearly want to move in the same direction, but this is the first step on that journey.

What we have done now is build up relationships that we will be taking forward in the next weeks and months to start to make tangible differences and to talk about what that data sharing looks like. How do we get bits of law enforcement to work together? Going back to my analogy about the value chain, how do we work with those tech companies, telcos and others to understand what we need from them? This is the start of what I hope will be really fruitful.

Q402 **Chair:** We are going to have some questions on social media companies and what exactly they are doing or not doing.

Mr Cheeseman, could I ask you about the problems with prosecutions? Where there is public sector fraud, the general public would want to see as many prosecutions brought forward as possible, but we know that less than 1% of fraud offences against individuals are prosecuted by the CPS. The UK criminal justice system is already in severe difficulty. There are huge backlogs of cases. Can you offer any reassurance about bringing people to book for public sector fraud?

Mark Cheeseman: Of course. A few weeks ago, you heard from Richard Las from HM Revenue and Customs, which is looking at fraud against the public sector and the tax system, about some of the action they are taking on prosecuting those who commit fraud.

The Department for Work and Pensions also prosecutes people who commit fraud, working with the CPS. Prosecutions happen and action is taken. Historically, it is not something we have collected data on across the whole public sector, but the Public Sector Fraud Authority, since coming in, has now started collecting data, public body by public body, on the level of prosecutions and the pieces that are going on there. That is quite a big task, with hundreds of public bodies that we are looking at. That will enable us to bring this picture.

The thing I would like to just draw out is that, while some prosecutions are important to bring people to justice and to create a deterrent effect, investigating economic crime is quite expensive. Again, you heard this from Richard Las. There are a range of different approaches that we take. First, we will do compliance work, and Government Departments will do work exploring other types of sanctions in their policies and contracts that they can use where they suspect fraud.

Secondly, one of the real focuses of the Public Sector Fraud Authority is on how you prevent. How do you take those learnings to build better systems and stronger processes, and to design out as much of the fraud as possible? In 2023, the Public Sector Fraud Authority launched a risk, threat and prevention service that works with public bodies to really understand those risks and get more prevention in, using tools like data and data sharing, as you have touched on already.

Q403 **Chair:** Are you able to point the Committee to Departments or organisations that are doing well at finding, investigating and prosecuting fraud?

Mark Cheeseman: The two big parts of the public sector that focus on that are the Department for Work and Pensions and HM Revenue and Customs. They have 84% of the resourcing, and that is where the main risk and threat lies, so that makes sense and is quite aligned. If I were looking at the places that are really pushing on that, it would be there first and foremost.

Outside that, we publish a fraud landscape report every year, which details what level of fraud is being found. The Government have an active policy to find more fraud because, by finding fraud, we can deal with it better. We can better prevent. We can better understand the attacks.

We have steadily increased the level of detected, recovered and prevented fraud since that started being reported. That report will break down by Department where fraud is being found. Once we have the prosecutions data, we can then align that to that as well.

Q404 **Chair:** You do not have the prosecution data yet?

Mark Cheeseman: No. We have started collecting prosecutions data this year. What was collected previously was the level of detected fraud to the civil balance—where someone suspected, on the balance of probabilities, that there may have been fraud.

Q405 **Chair:** What do you have to say about the huge backlogs in court cases?

Mark Cheeseman: That is a wider challenge in the system. There is a challenge there. I know that the Government are working on it. It is not one of my areas to look at, but I would come back to the point that it is not just about prosecutions through the criminal system. There are a range of actions to deter fraud, and we will not deal with the volume of crime against the public sector or other sectors just through that route. It is about diversifying the approach.

Q406 **Chair:** The Committee accepts that you need to prevent. We know we cannot prosecute our way out of this, but for the public sector, the general public would want to see people brought to book, particularly for public sector fraud. That seems very clear to me—thank you very much.

Mr Ephgrave, the Government have said that they are going to amend the Crime and Courts Act 2013 so that, in the same way that the NCA has power to direct the police in relation to serious and organised crime, the director general of the NCA will be able to direct you on matters relating to the investigation of suspected incidents of serious or complex fraud, bribery and corruption. Could you say something about that? How will having that direction affect the Serious Fraud Office?

Nick Ephgrave: It is a recent amendment, as you rightly say. A lot of thought has gone into it. If I can use an analogy, it is a bit like having, by a fire escape, "Break glass in an emergency." It is that kind of provision.

I certainly am in discussions with my colleagues in the NCA. We are very much of the view that this is something that really should not have to be used, because we ought to be getting around the table. The National Economic Crime Centre is the place where these discussions would naturally take place. We should be able to get around the table and find, between us, the right way to deal with whatever the nature of the threat is. I am certainly not slow in coming forward in terms of accepting referrals from other agencies. I have a good track record in the short time I have been here.

Q407 **Chair:** Why are they thinking they need to bring that in and amend the Act? Why are the Government deciding to do this if it is only in really difficult circumstances, if you are saying it is all fine and you take referrals?

Nick Ephgrave: It is sensible to have a provision should there be a disagreement, but at the moment we have not reached that position. I would like to think that the collaborative approach I am taking, working not just with the NCA but with domestic police forces, would mean that we will not need recourse to such a mandation, but it is always sensible to have a provision if that were ever to happen.

Q408 **Chair:** Is this historic, then? Have there been problems in the past before you arrived?

Nick Ephgrave: I am not aware of any, but I have been in the job for five months, so my knowledge of the deep history of the SFO is limited.

Q409 **Chair:** You have only been there five months. Do you think you have enough resources to effectively investigate serious fraud?

Nick Ephgrave: My job is to make the best of what I have. I have a team of about 600 people and my job, as defined in the statement of principle, is very specific. It is about international bribery and corruption, and serious and complex fraud where there is significant harm intended or caused to the public in general, the economy and prosperity of this country, or its reputation as a safe place to do business. It is a fairly tight set of criteria.

Of course, one could always do more with more, but that is the same for every public service—every public service would say that. The thing I need to focus on is driving the best outcomes I can with whatever I am given. I will always articulate the case for why it is sensible to invest in the SFO.

It is right to say that we provide good value for money. If you look at our return on investment for the last five years, it is about three to one. For every pound that has been invested in the SFO, we have delivered £3 of benefit back to the Treasury, so we are certainly a good value-for-money organisation, but my principal aim is, with whatever I have, to make sure I deliver the most I can with it.

Q410 **Chair:** You have just mentioned making the best of what you have and whatever you are given. That does not exactly sound to me as if you are saying, “Yes, I have sufficient resources to do the important job that I have been given.”

Nick Ephgrave: We have heard the scale of the fraud threat. I have to apply criteria and I have to prioritise cases, because I have a limited amount of resource. As I said, that is the same for everyone who runs a public service. There is always an argument to ask for more. You can do more with more. That is an obvious point to make, but I am very alive to the fact that there are competing demands for a limited amount of money.

I probably used a clumsy phrase. I am trying to say that I need to make sure that the resources I have under my command are directed in the most efficient and effective way. That is probably a better way of saying what I tried to say earlier.

Q411 **Chair:** Do you get any of the additional resources through the fraud strategy? Of the 400 investigators, are any of those going into your organisation?

Nick Ephgrave: The national fraud squad that has been referred to, with those 400 investigators, is a separate entity. They sit in a different environment, but we can work alongside those people; it does not mean that we cannot work together. It is a relatively new innovation, as we have heard, so we are working to see how that can help us, but they are not directly coming to the SFO.

Q412 **Tim Loughton:** Mr Fell, yours is a pretty new role, and you took over quite quickly from your predecessor. Is it a meaningful role?

Simon Fell: I very much hope so.

Tim Loughton: So do we, but is it?

Simon Fell: Yes, I think so. We have this fraud strategy. It needs delivering. My job is to make sure that we keep that motoring along, but more than that, it is about making sure that we are looking at new opportunities and that we continue to move as the threat moves too.

Q413 **Tim Loughton:** With respect to your own position, the Government have appointed lots of champions over many years, although I have not been a champion of anything officially. There is no real official status to it, is there? What do you have access to that any other MP does not effectively have access to?

Simon Fell: I have a team of fantastic officials, some of whom are sat behind me right now, and the weight of the Home Office. I have been empowered by the Prime Minister to work with the Home Office, the Ministry of Justice and across Government to bear down on the challenge of fraud.

I have to say that in the short time I have been in post, I have not found any challenge in getting doors opened or finding people who are willing to work with me, because this is a priority of the Government.

Q414 **Tim Loughton:** What does access across Government mean though? You are primarily working with the Home Office, are you not? Are all your officials based in the Home Office?

Simon Fell: Yes.

Q415 **Tim Loughton:** Yet fraud is a big responsibility within the Treasury and various other Departments as well. Practically, how real is joined-up Government across those Departments? Was this really a Home Office-driven thing?

Simon Fell: It is a Home Office strategy, but it is a Government strategy as well. There are agreed measures in there, so it is about getting them over the line and making sure that where there are points of friction, I can reach out and talk to other Ministers and make sure that they are aligned.

If we are seeing a particular challenge, I can bridge that gap, and I can take some of the weight off the Security Minister and the rest of the team and just focus on fraud for the PM.

Q416 **Tim Loughton:** Notwithstanding your own suitability for the job, should it really be a ministerial post? Should we have a full-blown, cross-cutting Minister for fraud at a high level?

Simon Fell: There is a very strong case for that. I am not looking for that job, and I am not entirely sure it is within your gift to give it to me either.

Tim Loughton: We could give you a good write-up in the report, perhaps.

Simon Fell: That would be very much appreciated. In all honesty, while there is a clear value in connecting Treasury and Home Office, I am not seeing a disconnect there since I have been in post. We are aligned on this strategy. The whole of Government is aligned on this strategy, and the last couple of days have shown that. We have had representatives from across Government working with international partners. No one has been dragging their feet on getting this stuff over the line.

Q417 **Tim Loughton:** What have been the takeaways from this great fraud summit that was taking place over the last couple of days? Has it achieved anything apart from a few communiqués and photo opportunities?

Simon Fell: The key thing is that we now have international partners who are willing to take those next steps with us on better protecting victims, looking at international data flows, going after the criminal gangs responsible, and finding common ground on new areas like tech where we can work together and agree a common approach to how we engage with some of these companies. None of that was in place before, and it is up to us now to take that forward.

Q418 **Tim Loughton:** You said earlier that we have some good data-sharing schemes, of which you were a part but in the private sector. Do you think that the public sector is learning enough from the private sector, or are they two very different spheres?

Simon Fell: I am straying somewhat out of my brief if I answer that, so Mark may want to step in.

Mark Cheeseman: I am happy to come in on public sector fraud and how we deal with that, and working with the private sector. We absolutely are learning from the private sector. Could we do more? Will we challenge ourselves to do more? Always.

An example is our partners in the Public Sector Fraud Authority. We have gone out and openly procured partners. We have a range of partners from the private sector. We have had secondees into our organisation from the banks. We have an advisory panel that advises the leadership team, which Simon and other people from other sectors and other countries sit on, to bring this richness of experiences from other spaces and this challenge to us and to the public sector in how we are doing it.

Building capability is so important. It is about how we build the capability and people to understand and deal with fraud in the public sector. The Government counter-fraud profession itself has a cross-sector advisory group on which the private sector, the charity sector and other sectors sit to advise and challenge us on how we are building that, and to make sure we are not just building it with blinkers on, but that we are looking out and thinking about those broader experiences.

Q419 **Tim Loughton:** What good lessons and good examples have we adopted from the private sector, which has probably been doing this more intensively for longer than it has been on the radar of public sector agencies?

Mark Cheeseman: The use of data and analytics is one lesson from the banking sector and other sectors. We do quite a lot with data and analytics. We have just announced that we will have £34 million more in investment for the Public Sector Fraud Authority to do more with data and analytics to find and prevent fraud. That is very much building on the experience we have seen in banking, insurance and other sectors as to how they have harnessed their data to look for and prevent fraud.

Q420 **Tim Loughton:** Going back to the old days when I was in the City and involved in the financial world, in the days where we had a partnership stock exchange, we had something called the stock exchange mutual reference society, which was a very early, basic forerunner of anti-fraud whereby, whenever we took on a new client in stockbroking, we had to refer them to the stock exchange mutual reference society so that any other stock exchange financial firm could check their records. If they had been somebody who had legged it owing them some money or had done some suspected insider trading or whatever it may be, we were tipped off: "You shouldn't deal with that person". When there was corroborating evidence, it could be referred to the police if there were suggestions that this person was potentially a criminal as well.

It worked really well. This was before the days of technology and everything, but it worked. Now that we have technology and all the AI assistance that we have, that sort of thing should be so much easier, should it not? Yet it is such a bigger problem. Are we missing the wood for the trees because we are not sharing and comparing data with the most relevant agencies?

Mark Cheeseman: Again, we could do more of it. It is a big world with a lot of public bodies and private sector organisations looking at it in different ways, so I am not saying we cannot do more, but there is a lot of activity going on.

One of the challenges with public sector fraud is the diversity of it. It could be welfare fraud, tax fraud, fraud against grant schemes, internal fraud in the public sector, or fraud on procurement or contract management. It is incredibly diverse.

On the use of data from other sectors and the example you gave, we did some work on sharing known fraud data with other sectors and looking at how we could use that. Where were known fraudsters in the system? It is very helpful in some cases, but known fraudsters access the health service; they access welfare benefits if they are entitled and if their earnings are of such. We have to use that data and those tools in a way that is targeted towards the problem that we experience and the diversity of it in the public sector.

Q421 **Tim Loughton:** Mr Ephgrave, the Serious Fraud Office deals with serious fraud—the clue is in the title—but the vast majority of fraud is affecting our constituents. Every day, people are scammed out of hundreds or thousands of pounds in paying for services or goods that do not appear. Are you only really concerned with the big stuff? Are we then missing resource and application to the more common stuff, which some might say causes much more disruption and misery to ordinary people than to corporates or whoever, who take it in their stride?

Nick Ephgrave: You are right to say that we deal with a small proportion of the totality. That is absolutely right.

I mentioned earlier the statement of principle by which I need to decide which investigations we take on and which we do not; that statement of principle talks about harm caused or intended. I have to think about not so much individuals, but the collective harm to the public in general or the economy of this country, or its reputation as a safe place to do business, which takes me into the bribery and corruption part, which is not necessarily relevant here. The final criterion that has to be met is that the nature of the fraud is such that only the SFO, with its specialist skills—I will come to that in a minute—and powers can deal with it. All those criteria need to apply before we take an investigation on.

To give you an example of the scale, there is a recent example of an investigation we adopted, which I can talk about because it is in the public arena: the collapse of the Safe Hands funeral care service, where 46,000 ordinary, hard-working people who were mostly retired and thought they were making a very safe and prudent investment to provide for their family after their death had their money stolen. That is the kind of collective harm that will bring that fraudulent activity into the world that I am interested in.

The other thing to say about the SFO's specialist skills, which is not always apparent and you would not necessarily know if you had not read up on it, is that we are the only organisation that has both investigative and prosecutorial powers. As the director, I am charged with deciding both which investigations I take on and which, having investigated, I then prosecute. My cases do not go to the CPS; they are entirely handled in-house. That was something that Lord Roskill devised way back in the 1980s when he reported on the then Government's response to fraud.

Q422 **Tim Loughton:** Do you think that works well?

Nick Ephgrave: The multidisciplinary team is a really important element of what we do, because our cases necessarily take quite a long time. Almost all our cases are multi-jurisdictional. We have already heard from Mr Fell that so much fraud is international. That is particularly the case for the types of fraud I deal with, so having forensic accountants, lawyers and investigators, as well as data analytic experts and tech people, within the team provides me with the best opportunity to exploit the opportunities that the investigation presents, without having to go and find those people, which you might have to do if you were in a domestic police force.

Q423 **Tim Loughton:** Is that a model that the police force could look at, if it has worked so well with you?

Nick Ephgrave: The model was designed to cope with the very top-end, complex and lengthy investigations that we have and the multi-jurisdictional nature of them.

Of course, in the volume crime world—as a former chief constable, I understand this—one also works very closely with the CPS, but they are not part of the same organisation. By design, there is absolutely a corridor between the two organisations. The investigation is conducted by the police; it then goes to the CPS to consider the evidence and make a decision. That model works very well for the vast majority of offending in this country. The specialism I have was designed to deal with the particular complexities of serious and complex fraud, bribery and corruption.

Q424 **Tim Loughton:** Sure, but do you measure that compared to the police and the CPS? We have had a lot of experience with the police and the CPS, not least with sexual crime and the low prosecution rate, and considering whether that is down to the police not investigating properly and passing on poor cases or the CPS not properly getting the information across or whatever.

Do you think that your success rate is due to a much higher number of the cases you investigate then ending up in prosecutions, successful or otherwise? Or is your threshold higher so that you do not investigate so much or proceed with it unless it is much more serious, or vice versa? I am just trying to get a measure of how it compares when it is a one-stop shop, or whatever you want to call it, that you are operating.

Nick Ephgrave: It is a very interesting question, because whenever you specialise and create a group of people whose sole job is quite well defined and quite specialist, and you invest resources and expertise in it, you tend to get better results. That is what differentiates any specialist police unit or my teams from the generalist PC who goes to investigate a low-level theft or something. They are a one-person band; I have the advantage of having a bunch of legal, forensic and investigative experts who can focus all their intellectual energy, effort and experience on this one case.

That tends to produce better results, but of course it is an expensive model, which means that we can only take on a limited number of cases. To try to expand that model into volume crime would create enormous resourcing implications.

Q425 **Alison Thewliss:** I have some questions about social media companies. We have heard lots of evidence not just that frauds are being committed via social media, but that organised crime is actively using social media to perpetrate those crimes. I wonder if you could each comment on what responsibility the social media companies ought to be taking for what is being perpetrated on their platforms.

Nick Ephgrave: I probably have a particularly limited view on this. I am an investigator and a prosecutor, so we tend to respond to what gets referred to us, but we do see the use of social media as a propagator for some of the scams and investment frauds, in particular, that we see.

The point that was being made earlier about prevention and education in that sector is really important. I was lucky enough to be at the global fraud summit, and we had a number of representatives from the social media companies who recognised their responsibilities to do what they could to provide security to the people who use those platforms.

There is always more that can be done. An interesting thing to think about is whether the new "failure to prevent fraud" provision in the Economic Crime and Corporate Transparency Act that has just been passed would have the reach to go into companies that provide services that are not necessarily financial services but are a platform for the propagation of fraud. That is something that will need to be thought about and tested.

Q426 **Alison Thewliss:** The risk assessment of the "failure to prevent fraud" offence suggests that very few cases were brought before the courts on that. Do you think that is going to be effective enough?

Nick Ephgrave: It remains to be seen. It has only just gone into statute. I am determined to be the first person to do it—that is my goal. I cannot predict which case it will be, but I am looking for it right now.

Simon Fell: You are absolutely right. These platforms are used by criminals. We know that fraudsters operate on them—they target people on them. This is not just a social media issue; we see it across all kinds of industries, but we also see an incredibly wide range of frauds running across these platforms.

We heard compelling evidence about romance fraud and the impact that that has on people's lives. That is a very different crime from someone trying to drive you off-platform to a secure communication service so you can then send money as part of a financial fraud of a different sort. We need to tackle them differently, but it is about understanding the signals in the system, and it is about getting these companies to come to the table, act responsibly and work with partners in law enforcement and across other industries, and with Government too.

We are in a reasonable place with them. We certainly have a long way to go, but we signed this online fraud charter a few months ago with them. A wide range of organisations, including some of the biggest tech companies in the world, voluntarily came to the table to enact measures that will take them time and effort, cost them money, and potentially drive down some of their revenue in doing so. We have to take them at face value on that.

In two months' time, when the charter kicks in properly, let us see what the results are. If they do not deliver, that gives us an opportunity to go back and have some more robust conversations with them, but we also have the Online Safety Act coming in at that point, where the provisions that Ofcom is consulting on at the moment will kick in. Then there are the opportunities for quite substantial fines to be levied against these companies if they do not act properly on fraud and some of the other stuff we see on their platforms.

Q427 **Alison Thewliss:** You mentioned what will happen if they do not deliver. How will you be measuring that delivery against the charter?

Simon Fell: That is part of what I am doing at the moment. I am doing roundtables with all these tech firms, checking up on their progress against the objectives in the online fraud charter. We are looking at the metrics so that when they put in customer authentication or "two clicks away from reporting a fraud" in their system, we can get from them what that does in terms of changing user behaviour: what are they seeing in terms of the amounts of fraud that is reported?

This is the first step. If we do not see changes in the amount of fraud running across these platforms or in consumer behaviour in the way that we hope we would, or if we do not see less fraud on platforms, obviously we will be going back and having more conversations with them.

Q428 **Alison Thewliss:** What kind of consequences would you envisage if they do not see a change?

Simon Fell: This is essentially a dry run for them. If they do not get their house in order for this, they have the Online Safety Act provisions coming in, at which point there are potentially swingeing fines coming their way if they are not properly looking after their customers and trying to prevent fraud on those platforms.

Q429 **Alison Thewliss:** I have had the distinct impression that they were not taking this as seriously, and not just from evidence to this Committee. When I was on the Treasury Select Committee, we also looked at this issue. TSB said in evidence to us that in its sampling from Facebook Marketplace, a third of the adverts were fraudulent and Meta did not really recognise that. Is it a problem that they do not recognise what the banks are seeing?

Simon Fell: You will probably always find a discrepancy between one company and another and what they say they are seeing, but we have seen, for instance, a pilot up and running between Meta and a couple of the banks where they are sharing data. They are trying to identify where fraud is happening and better drive that down.

It is early days, but they are getting some decent results from that. We want to see that working across the whole system. They recognise the challenge they have; otherwise they would not have signed up to this. Otherwise they would not be leaning in to the Online Safety Act with some concern. They have a very short period of time now to get their houses in order and demonstrate that they are moving in the right direction and taking this seriously. If they do not, they will have the full force of the law holding them to account.

Mark Cheeseman: It is not an area of my direct responsibility, but the public sector does have an angle on it, because these platforms can be used either to share methods to attack the public sector or to impersonate the public sector.

You heard last time from Richard Las about some of the work that HMRC has been doing in protecting the brand of HM Revenue and Customs, and how this has had a good impact in that space. From my point of view as a fraud expert, all sectors have a role to play. I am very supportive of the wider effort in the fraud strategy to encourage all sectors to have a role to play in protecting their users and, in the public sector's case, the public.

Q430 **Alison Thewliss:** There was a "File on 4" documentary a few years ago about people being recruited to be company directors via a Facebook group. That is obviously related to the vulnerability of UK corporate structures. Do you think HMRC is alive enough to this?

Mark Cheeseman: The Economic Crime and Corporate Transparency Act is reforming Companies House. That is one of the tools we were talking about earlier. One of the tools we have developed is sharing data from policing, the NCA and sanctions lists to help Companies House to look at how, under the Economic Crime and Corporate Transparency Act, they make that register more robust.

Q431 **Alison Thewliss:** Given the scale of information that is quite clearly guff on the Companies House register, is enough resource going into tackling that?

Mark Cheeseman: That would be a question for that Department and for Companies House itself. We are there to assist them with tools that we can develop.

Q432 **Alison Thewliss:** I am quite concerned about the corporate structures facilitating fraud. We saw that through covid, with companies being set up in order to get furlough payments or PPE contracts. Is enough scrutiny put upon that at the moment? Have we learned things from that experience?

Mark Cheeseman: We are certainly learning from that experience. The data analytics platform that I have just talked about was developed during the pandemic to deal with the types of frauds and challenges we were seeing, and part of the investment is now to create that to use in a business-as-usual setting to have more impact. We are certainly learning our lessons and trying to do more.

I go back to what was said before. We do not have a static adversary; we have an adversary that will be agile. We will move the defences, and they will look to attack in a different way, so we cannot just say, "We are doing this—job done." It is always going to be a further effort to try to understand how we may be attacked, and then to continually improve our defences.

Q433 **Chair:** Mr Fell, one of the concerns of the Committee is around terrorism and terrorists using fraud across the piece. We are a bit concerned that that is not getting the attention it deserves in all the documents and strategies that the Government are putting out. What do you say about that?

Simon Fell: The fraud strategy directly acknowledges the link between fraud and more serious and organised crime, including terrorist financing. That is what the National Economic Crime Centre within the NCA looks at.

We talked about data sharing earlier. Data from industry, Government and law enforcement sits there, and it is interrogated by investigators so that they can make those links. You can see that what might be considered to be relatively low-level fraud, connected through money laundering, people trafficking, or sometimes modern slavery or county lines drugs running, is essentially a criminal enterprise running to fund some form of nefarious activity. Their job is to piece all this data together and then go after the worst offenders.

It is recognised in the strategy. It is a clear function of law enforcement to do that, and they have the people and the resource to go after that as well.

Q434 **Chair:** You are saying that you are satisfied that the Government have a handle on this.

Simon Fell: I am satisfied that the Government are very clear that this is an area of concern. There is a function of law enforcement that looks at this, but we can certainly always be doing more.

Q435 **Alison Thewliss:** I have a brief question for Mr Ephgrave. I have heard in the past that it is difficult both to recruit and to keep people on public sector wages who have the expertise you require to go after these folk. Is that a concern for you?

Nick Ephgrave: It is a concern. It is something that does not just affect the Serious Fraud Office. We have to compete with the private sector; we have to compete with private law firms that can pay more money than us.

What I try to sell to my people is the mission. It really gets under your skin. If they really believe in what we are doing, there are people who are very happy to accept that they are not going to get paid quite as much to come and work for the SFO as they might if they went into a private law firm.

There is something I want to generate in this country that is very effective elsewhere. I have just come back from visiting colleagues in the US, and they have this system there. There is a much greater in-and-out movement of lawyers, in particular, coming into the SFO to gain some public sector experience to contribute to the fight against serious and organised crime and fraud, then potentially moving back into the private sector, and then some years later coming back in again. There is not such a great crossover as there is elsewhere, and that is something I am quite keen to promote.

Q436 **Alison Thewliss:** In the US, I believe they are able to keep some of the proceeds from the crimes that they prosecute as well. If you were to go after a big organised crime gang, you could keep some of the money that you get back from that, whereas in the UK it is more of a risk on organisations like you to take those cases. It would cost you more money to prosecute than you would ever see back.

Nick Ephgrave: Yes, but we participate in asset recovery, and we benefit from whatever we recover. We have an arrangement with the Treasury that I can provide you written details on. It is based on the

ARIS programme, which is the recycling of proceeds of crime. We benefit from that, as do all law enforcement agencies that recover assets.

The general point about recruitment and retention is definitely an issue that we have grappled with in the Serious Fraud Office over the years, and I am very keen to bring some new thinking to that.

Chair: May I thank all three of you for attending this morning? It has been very helpful. We will now move on to our panel with the Ministers.

Examination of witnesses

Witnesses: Rt Hon Tom Tugendhat MP, Baroness Vere of Norbiton, Anna Harvey and Duncan Tessier.

Chair: Welcome to our second panel this morning. This is our last session in our inquiry into fraud. May I ask you to introduce yourselves?

Tom Tugendhat: I am Tom Tugendhat, the Security Minister.

Baroness Vere of Norbiton: I am Baroness Charlotte Vere, the Treasury Minister responsible for economic crime.

Anna Harvey: I am Anna Harvey, a deputy director in the financial services group in the Treasury.

Duncan Tessier: I am Duncan Tessier, the director for economic crime at the Home Office.

Q437 **Chair:** Welcome. Perhaps I could start with you, Minister. Why has it taken 17 years to get the Government to take fraud seriously? I note that it has been 17 years from the publication of the fraud review in 2006 to the fraud strategy we got last year.

Tom Tugendhat: That is an excellent question. I am afraid I was still in Helmand in 2006, so I cannot answer it.

Q438 **Chair:** You speak for the Government.

Tom Tugendhat: I do, and that is why in the past year, since I have been in post, we have introduced the fraud strategy and we have made the difference that this Committee has quite rightly been asking for.

As you know, we have also introduced a new national fraud squad and a national fraud intelligence unit. We have organised a fraud charter, and up until yesterday there was a global summit as well. We have been doing an awful lot in the year that I have been in place. I am afraid I cannot answer for the Blair or the Brown Administrations, and I was not there for the coalition Administration from 2010 to 2015. I am afraid I am somewhat limited in being able to answer, except for the last year or two.

Q439 **Chair:** Just for clarity, in 2006 a Labour Government was in power, but from 2010 there has been a coalition, but Conservative all the way through, so it has taken quite a long time for the Conservative Government to get a grip on this.

Tom Tugendhat: That is an absolutely fair point. The Liberal Democrat-Conservative Administration that was in power then would have looked at this, no doubt. I am afraid, again, that I find it very difficult to answer because I was still a soldier.

Q440 **Chair:** Do you think that covid had an impact on this? Is that why the Government woke up: because fraud increased during covid?

Baroness Vere of Norbiton: Can I just make a couple of comments on your first question, because I do not think it actually gets to the heart of the matter? The Government have been taking fraud seriously for quite some time. What the fraud strategy did was bring together all the different strands.

If there is one thing I learned from the global fraud summit yesterday, it is that fraud is complicated and international, and pervades all sorts of elements of our society and economy. The fraud strategy was an opportunity to bring together all those strands. One only has to look back to 2017, for example, when the Payment Systems Regulator brought in the requirement to reimburse victims. Lots of things have been happening. You know the economic crime plan; that is the second economic crime plan. Economic crime is a big picture, but part of that is fraud.

There has been a steady progression. There has been lots of good work happening in lots of different places, as you will have heard from previous people. It is quite a fragmented picture, and the fraud strategy brings all that together.

Q441 **Chair:** Bits and pieces have been happening over time.

Baroness Vere of Norbiton: It is slightly more than bits and pieces.

Q442 **Chair:** The fraud strategy brings it together?

Baroness Vere of Norbiton: It is an opportunity to bring it together, following on from economic crime plan 2. Cutting fraud was one of the three outcomes from that.

Chair: It is fair to say that fraud has been given quite an impetus with your arrival, Minister.

Tom Tugendhat: I would hope you would recognise that.

Baroness Vere of Norbiton: Yes, absolutely. He gets all the credit.

Tom Tugendhat: Thank you very much. I am very grateful.

Q443 **Chair:** I saw the comment that you gave yesterday, Minister, from the global fraud summit. You say, "The action we've taken has already reduced fraud by 13% in England and Wales".

Tom Tugendhat: That is right, yes.

Q444 **Chair:** The Committee is rather concerned about the statistics around fraud, because what we have discovered in our inquiry is that the vast majority of fraud is not reported, so while there is a 13% drop in what has been reported, at least one in seven offences are not.

Tom Tugendhat: Can I address that?

Chair: Yes, I want you to address that, because I am just wondering if it is a little complacent to think, "Fraud is going down. We must be doing everything right," when the vast majority is not reported.

Tom Tugendhat: I completely accept your point. Of course the statistics cannot be absolutely certain, but they are indicative of a direction that is important.

You mentioned covid earlier. It is an important thing to mention, because a lot of the world went online during covid, in a way that people could have done before but a lot of them did not. We got used to shopping and trading and doing a whole bunch of things online that we had previously done in person. It is true to say that we saw a rise in online fraud, which for a lot of people made fraud a lot easier, sadly, and made a lot more people victims of fraud.

It would be untrue to pretend that every single fraud crime is reported. We know that that is not true, but we also know that the direction during covid was up. We recorded it. We did not record 100%, but we did record it. Since then, we have seen it down. Is it down exactly 13% or is it down in the direction of about a little over a tenth? I would probably stick to a little over a tenth.

The statistics are accurate in the sense that this is reported crime from the crime survey for England and Wales which, as you know, is the most reliable reporting of crime. Your point stands, which is that that cannot be absolutely nailed on as every single crime in the United Kingdom, but it definitely demonstrates the direction. Just as the previous reports and the other statistics I am sure you could mention would demonstrate a trend upwards, this demonstrates a trend downwards. A lot of that, as you know, is down to the work that not just the Government but many companies have done. There has been a huge amount of co-operation with companies around the United Kingdom, including banks, tech companies and telecoms companies, which has made that difference.

Q445 **Chair:** One of our concerns is how easy it is for people to report fraud, and the problems with Action Fraud and the new way in which Action Fraud will operate. We were particularly disappointed when we heard evidence on 28 February that the new system will only be operational from the end of the year. Why is that? What role have you played in making sure that it is up and running as quickly as possible? We know that that is one of the problems: people feel that there is no point reporting.

Tom Tugendhat: You raise an important question. It is worth coming back to the fact that there is a difference between the effectiveness of Action Fraud and the reporting of crime that would come through Action Fraud. Anything that is reported through Action Fraud would count as one of those crimes in the crime survey for England and Wales, so that would not affect the statistics.

Your point about Action Fraud still stands, and it is an issue that we have been addressing, which is why we have asked the City of London police to deal with this. We have given them £30 million, and we are putting a huge amount of encouragement, if you are being positive, or pressure, if you are being slightly more negative, on the City of London police to encourage them to make the changes that we need to see in Action Fraud. I would like to see them happen yesterday, but as you know, when bringing a major national campaign like this together, you have to make sure that you are bringing all the police forces that need to co-operate with it, and not simply the City of London police, which of course has expertise and the lead on fraud in the United Kingdom.

Q446 **Chair:** Having this new, revamped Action Fraud is one of your flagship bits of the fraud strategy, is it not? I do not quite understand why there are delays, because this is not new stuff. We have always had police forces whose agreement you have to get to do various things with. Why is there a delay?

Tom Tugendhat: If I may, the flagship part of our fraud strategy is the sort of things we were talking about yesterday and the day before. It is international co-operation and the co-operation between companies, between companies and Government, and between companies, Government and law enforcement. That is really the flagship bit.

Chair: This Committee is particularly concerned about the effect on victims of fraud.

Tom Tugendhat: You are absolutely right to be.

Q447 **Chair:** That has been one of our main reasons for doing this inquiry. Action Fraud is a very important part of victims being able to report and feeling something is going to be done. The problem for the Committee is that we were told that this was going to happen, and now we are told that there is a delay. It just does not feel as if there is a focus on getting this right for victims.

Tom Tugendhat: If I may say so, you have been absolutely leading in focusing on victims, and I pay huge tribute to your work on this. One of the things that you have regularly said about victims is that it is better to prevent anyone from becoming a victim, and it is one of the issues that you have registered. Taking your lead, that is exactly what we have done. We have focused on prevention; we have focused on making sure companies come together to prevent fraud; we have focused on helping individuals to understand the threat of fraud.

You will be aware of the campaign that we have just started, "Stop! Think Fraud". We have worked on bringing together partners from around the world because, as you know very well, some 70% of fraud is connected to overseas, so that joint action is incredibly important.

Q448 **Chair:** It is not an either/or. You can do both. You can do that international work, work with companies, do the prevention work and all that, but you need to have a functioning way of allowing victims to report fraud—and you do not have that.

Tom Tugendhat: I would not agree with that statement. We have a functioning of reporting fraud, and Action Fraud does record and report fraud. There are challenges with Action Fraud on further action—you are absolutely right—and that is why the things that make the biggest difference to Action Fraud now and help the capabilities that we would have wanted it to do to respond are the national fraud squad and the national fraud intelligence unit.

Q449 **Chair:** You keep deflecting away from Action Fraud. All I want to know is why something that is so important is being delayed.

Tom Tugendhat: Madam Chair, forgive me: I am not deflecting away. I am saying that Action Fraud is one element within a wider strategy.

Q450 **Chair:** I am asking you about that one element. I understand all the rest. I am asking you, as the Minister responsible, why Action Fraud in its revamped, all-singing, all-dancing model, is not up and running. Why are we having to wait until the end of the year?

Tom Tugendhat: What I am explaining is that it is up and running, largely. It is not rebranded—that is certainly true—but it is up and running, because the thing that Action Fraud brings together is the ability to respond to fraud. That is the national fraud squad. It is the training of the different fraud leads in various police forces. That is 100 extra police officers, who we are hiring at the moment. It is the national fraud intelligence unit, which is already up and running. All of these sit behind the brand that is Action Fraud.

You are right in saying that the brand could do with a change. That is what we are working with the City of London police on, but the capabilities that it brings together are being updated, even now and even without the brand change.

Q451 **Chair:** I still do not understand or have an answer as to why there is a delay. We were told on 28 February that the system will now be operational from later this year.

Tom Tugendhat: Forgive me, but it is operational; it is just operational under an existing brand rather than a new brand.

Q452 **Chair:** Sorry, I am really confused now. We were told that by the end of the year there would be a new system of Action Fraud that would work better. You are saying it is already in operation.

Tom Tugendhat: A lot of it is.

Q453 **Chair:** Why is all of it not? That is my question to you, Minister.

Tom Tugendhat: It requires a lot of co-operation across police forces. We are working on getting that in place.

Q454 **Chair:** What is the problem with the police forces? Are they not responding to you? What is the issue?

Tom Tugendhat: All of them have many priorities. You do not need me to tell you this. They have many priorities and we are bringing them together. It just takes time.

Q455 **Tim Loughton:** Mr Tugendhat, to come back closer to home for your responsibility, what came out of the summit of the last two days regarding the link between fraud and the financing of terrorism?

Tom Tugendhat: The summit did not focus so much on that. We would normally do that in a more closed setting. The summit that we have just had in Lancaster House was much more to do with the connection between social media, tech companies, telecoms companies, law enforcement and Government, and making sure that we kept each other's population safe. As one of the executives pointed out, it was largely the victim nations that were assembled rather than the nations that very often harbour fraudsters. That is what it was bringing together.

Q456 **Tim Loughton:** What is happening that is disclosable regarding combating fraud that is financing terrorism, that was not discussed in the last two-day summit?

Tom Tugendhat: There is an awful lot that we are doing on that. In many ways, it does not really require separate discussion, because they are the same techniques that lead to money going to terrorists, criminal groups, drugs groups or whoever it happens to be. In that sense, the participant is not the important bit; it is the technique. What we are trying to interrupt is the technique, in order to make sure that the moneys do not go to criminal groups, whether they are terrorist or whatever they happen to be.

The work that we were doing over the last two days—and, indeed over the many months before—is all about trying to interrupt that flow of money and making sure that we can put in various ranges of interruption, whether it is awareness at the earliest stage where a victim simply does not comply with an early request, whether it is interruption by technical means, or, indeed by the bank finally blocking a payment. That is what we were working on.

Q457 **Tim Loughton:** What successful interruptions have there been for combating finance going to terrorist organisations abroad?

Tom Tugendhat: I do not have those figures with me, but there has been an awful lot of interruption of fraud over the last few years. That is why we are able to say that fraud is down. To the Chair's position, the exact figures are very hard to be certain of, but according to the crime survey for England and Wales it is 13%.

Q458 **Tim Loughton:** Does fraud by terrorist organisations based in Syria, Iraq and other middle eastern countries get featured in the crime survey for England and Wales? It probably does not. Mrs Miggins of 1 Acacia Avenue, Warrington is not going to make any comment about how her funds have fraudulently gone to finance al-Qaeda or other organisations.

It is surely not part of that survey, is it?

Tom Tugendhat: She may not know, but the fact that she has reported a fraud would in fact qualify under the crime survey for England and Wales, whoever the beneficiary was.

Q459 **Tim Loughton:** How do we know, as you have just stated, that fraud across the board has gone down? We will take your word for it.

Tom Tugendhat: You do not have to take my word for it; it is the crime survey for England and Wales.

Q460 **Tim Loughton:** Yes, but, as we have just discovered in the conversation with the Chair, that is largely contingent on what is actually being reported, not what is actually taking place.

Duncan Tessier: Might I just interrupt on this particular point about reporting and the crime survey? Just to be clear, the crime survey is a statistical sample of 30,000 individuals across England and Wales. It is a representative sample. It does not suffer from under-reporting issues, because it is deliberately designed to give the full picture.

The under-reporting issue pertains to Action Fraud, where about 15% of frauds actually get reported to Action Fraud. That does not impact on our ability to understand the total volume of fraud, which is a very accurate measure through, as the Minister says, the crime survey for England and Wales. I hope that makes sense.

Q461 **Tim Loughton:** Let's have some examples of how fraud has been used to finance overseas terrorist organisations.

Duncan Tessier: There were a few examples that were provided in the fraud strategy, and there certainly are examples of that happening.

Q462 **Tim Loughton:** How does it happen? If I have been defrauded, how could some of my money end up with al-Qaeda or whoever it may be? How do you judge that it has ended up with terrorist organisations?

Duncan Tessier: I would not speak to a specific case, but generally the mechanism through which fraud money is moved around the world is through money-muling networks, often with many hundreds of accounts connected together. The money moves all around the world, is often cashed out through cryptocurrencies, and can ultimately end up with organised criminals or terrorists. The evidence that I have seen certainly does not imply a huge volume of terrorist financing connected to fraud. That is the evidence.

Q463 **Tim Loughton:** You do not think that terrorism is a major beneficiary of funding from fraudulent activity?

Duncan Tessier: I have not seen intelligence to suggest that it is a major issue. It undoubtedly does happen.

Q464 **Tim Loughton:** What proportion is it, roughly?

Duncan Tessier: I am not necessarily going to get into proportions, because I am not sure the intelligence is strong enough to get to that level. I can say that our assessments, where we have worked with law enforcement, do not suggest it is a major source.

Q465 **Tim Loughton:** The evidence from intelligence reports that I have seen, certainly with regard to middle eastern terrorist organisations during the caliphate, for example, shows that the three major sources of funding came from drug trading, antiquities trading, and online fraud and other forms of fraud. You are saying that the fraudulent part of that was actually pretty minor.

Duncan Tessier: The point I am making is about the total volume of fraud affecting the UK. We have talked about the scale. It is quite enormous. I have not seen intelligence to suggest that a large proportion of that is going to terrorist financing.

Q466 **Tim Loughton:** How do you know that? Where is the evidence to suggest that?

Duncan Tessier: The evidence is in the work that we do with the National Crime Agency, in particular, who have an assessment of the sources of fraud impacting on the UK. I have worked on those assessments.

Q467 **Tim Loughton:** When the National Crime Agency appeared in front of us recently to tell us that terrorism was closely linked with fraud, they were crying wolf, were they?

Tom Tugendhat: I would not say that they were crying wolf. I would merely say that we look at terrorist financing from the other end of the telescope. What we are discussing here is the perpetration of fraud against victims: individuals losing sums of anywhere from a few pounds to many thousands of pounds.

The difference is that when one looks at the other end of the spectrum, one sees currencies coming in from—as you rightly said—trading of illicit and illegal goods, or indeed from money transfers from different agencies, very often through cryptocurrencies and so on. Now, that money coming in may or may not be connected to fraud, but the effort that is put in there is very often to block the transfer of money rather than the origin of the money.

If Bitcoin is going into Raqqa, for one reason or another, the aim of our services is to stop that finance getting into Raqqa. Whether it has come from drug dealing, theft, fraud, or perfectly lawful sales and charitable contributions does not really matter; we do not want that money going into Raqqa, and we will seek to interrupt it. We will also do some analysis on where that money comes from. If there are links between fraud and sales of certain products, or whatever it happens to be, then we may get into that as well.

I do not think that is what Duncan was suggesting. He was merely suggesting that from a UK fraud perspective, the scale of fraud is sadly large, and a very small percentage of that large-scale fraud is going into terrorism—not the other way around, where the proportion of money going to terrorism may be disproportionately coming from fraud.

Q468 **Tim Loughton:** Let us come closer to home, where we might have some more detail on stats. Baroness Vere, the Committee has struggled to understand how joined up combating fraud is between Government Departments and agencies, and where the buck stops. Treasury has responsibility for money laundering and the Home Office has lead responsibility for fraud, with a lot of overlap between the two. How does it work in terms of joint working, information exchange and so on?

Baroness Vere of Norbiton: It is very simple. I will explain that. The overarching strategy is economic crime plan 2, which covers 2023 to 2026. This is the second version of that plan. It has three outcomes: the first is to reduce money laundering and improve asset recovery; the second is to combat kleptocracy and sanctions evasion; and the third is to cut fraud.

Going back to your previous question, of course it is all interrelated if you are trying to get money from the UK to Raqqa or whatever. It is always interrelated. You have money laundering in the middle. It all has to fit together and work nicely together. There are 146 actions in the ECP2, some that sit in the Home Office and some that sit in Treasury, and there is a governance structure that sits around that plan.

I have a really nice schematic here, which I might send to you after the evidence session, unless you have already seen it. At its heart is the economic crime strategic board, which is the Chancellor and the Home Secretary, who basically check strategic direction within the economic crime world. The thing that I am particularly struck by—and Tom and I did one very recently—was the joint fraud taskforce. It is when we bring together law enforcement, the private sector and NGOs. It is all about having those conversations about what we are taking forward, particularly in the fraud space. There is an economic crime delivery board. There is a public-private steering group. There are lots of different things.

The key thing about the economic crime plan is that it brings the public and the private sector together. The Government cannot do this on our own. We have to put the right incentives in place for the private sector, and that is what the system does. I do think we have a good way of working together. Could it be improved? Quite possibly.

Q469 **Tim Loughton:** Should we have an overarching Minister with cross-departmental responsibilities, as we do in other cases, with a lead on fraud?

Baroness Vere of Norbiton: I think Tom and I are perfectly capable.

Tom Tugendhat: It works better with the two of us than it would if there were a single Minister. The reason I say that is that, yes, of course there is an obligation on us to work together, and there is no question about that. We do have to work very closely together. Our Departments are actually looking at different things and have experience of different things.

It is quite right that the Home Office focuses on individuals, on police forces, on victims and on the criminality of it. It is quite right that the Treasury focuses on the finance aspects of it, the movement of money, the banking and the enabling architecture. The combination of the two makes it better. It is a little like Rome and Carthage. It is possible that you can teach the Romans to swim, but the Carthaginians demonstrated they were more able to take the land.

Q470 **Tim Loughton:** Yes, but the Carthaginians lost. That is all very well if there is a good exchange of information between the Home Office and the Treasury.

Tom Tugendhat: There is. Duncan and Anna are both here demonstrating that.

Q471 **Tim Loughton:** I am sure they are very impressive, but the presence of two civil servants does not mean that the whole system is working.

Tom Tugendhat: The reality is that the joint fraud taskforce is a very good indicator.

Q472 **Tim Loughton:** Can we come back to bank accounts? One of the things that has puzzled us—we have had a number of witnesses from the financial community—is that a lot of fraud happens via people being conned out of transferring money into a fraudster's bank account, which then gets cleared out.

Given how difficult it is to set up a new bank account—if you are an MP it is virtually impossible because of all the money laundering requirements, which have become more and more intensive; you virtually have to produce your blood group and various other pieces of lifestyle evidence before you are allowed to even start the process of setting up a bank account—how is it that bank accounts established by people who commit fraud, using those bank accounts as vessels to gain that money, are able to exist? Why are the banks and other financial institutions responsible for setting up those bank accounts unable to trace those people who have then committed fraud using their bank accounts? It is a Treasury question, at the end of the day.

Baroness Vere of Norbiton: Let me start, Tom, and you can fill in the gaps. First of all, from a politically exposed person perspective—which I presume is what you are referring to as a Member of Parliament—we did lay an SI towards the end of last year.

Tim Loughton: I am not interested in that; this is about ordinary people being caught with fraud. I purely said how difficult it is for anybody to set up a bank account, and most of all for us. We are not committing fraud, hopefully, otherwise we would not be here.

Baroness Vere of Norbiton: It depends what sort of bank account you want, because the nine largest bank account providers are obliged to provide a basic account to people, provided that they pass the due diligence checks and there is no suspicion of fraud. I am sorry, I am being slightly dim: I am not entirely sure what your question is.

Q473 **Tim Loughton:** If I were a fraudster, I would have to provide my credentials to Barclays Bank to set up a bank account. As a fraudster, by impersonating somebody from Barclays Bank or whatever, I get Mrs Miggins of Acacia Avenue to transfer her life savings into that bank account that I have set up, which I then empty and disappear. If I have had to provide my identity and credentials, which have been tried and tested by Barclays as is required under all sorts of money laundering regulations, how is it that they cannot then trace me and report me to the police in order to retrieve Mrs Miggins's money?

Baroness Vere of Norbiton: At that point the bank would provide the details to the police.

Q474 **Tim Loughton:** It does not, because it turns out that those people do not exist or have given fraudulent identities, which means that the bank has not done its due diligence. Presumably the Financial Conduct Authority is the responsible regulator for stepping in to make sure that the banks are doing their due diligence and that should not happen. Given that the FCA employs an awful lot of people and it costs £780 million to run, how does that happen?

Baroness Vere of Norbiton: The FCA is absolutely responsible for making sure that the banks do their checks. If there is a systemic failure within a bank to fulfil its due diligence, then of course there would be penalties levied against it.

Q475 **Tim Loughton:** Such as what?

Baroness Vere of Norbiton: There all sorts of levels: written warnings, fines, penalties, disclosures, all those sorts of things—the normal penalties that the FCA would normally give.

Q476 **Tim Loughton:** Are you the Minister responsible for the FCA?

Baroness Vere of Norbiton: It is an independent regulator.

Tim Loughton: Yes, but it comes under a Government Department.

Baroness Vere of Norbiton: It is an independent regulator, so it is accountable to Parliament.

Q477 **Tim Loughton:** Yes, but there is a responsible Department that oversees it as the intermediary between Parliament and that regulator. You are the sponsoring Department for any regulation and legislation affecting the Financial Conduct Authority. Are you that Minister or not?

Baroness Vere of Norbiton: No.

Q478 **Tim Loughton:** Who is?

Baroness Vere of Norbiton: Bim Afolami. Parliament sets the legislative framework in which the FCA operates. We have no operational control over the FCA.

Q479 **Tim Loughton:** In terms of its responsibility in cracking down on fraud, it is pretty important, are they not?

Baroness Vere of Norbiton: Yes, it is.

Q480 **Tim Loughton:** How many companies does it regulate?

Baroness Vere of Norbiton: It depends on which legislative regime it is under.

Anna Harvey: It is around 50,000.

Q481 **Tim Loughton:** It is 50,000, is it not? Do you know how many prosecutions there were in the last 12 months?

Baroness Vere of Norbiton: What for?

Tim Loughton: For fraud.

Baroness Vere of Norbiton: No, because what happens is that the FCA has no express power to prosecute fraud. It would usually only prosecute if it were furthering its statutory objectives. What would happen is that it would then pass on the intelligence to law enforcement, and what often then happens is that law enforcement would take that forward.

Q482 **Tim Loughton:** Yes, but it investigates. How many investigations does the FCA have at the moment?

Baroness Vere of Norbiton: I do not know. Do you know?

Anna Harvey: It is a very limited number. The FCA witnesses gave some evidence to you when you probed them on this a few weeks ago. If I recall, their answers were that they were really focused on the supervision and the prevention, and that they used their prosecuting powers in quite a limited way. I wonder whether this links to a wider point about prosecutions across the piece.

Q483 **Tim Loughton:** It is not prosecutions. That is why I am slightly surprised that you do not know those figures, Minister, not least because they were covered in the last session we had. One would have thought that as a Minister you would have read the transcript from the last session.

A really big concern that came out of that session is that a lot of this fraud, and certainly the volume fraud—the Mrs Miggins fraud, which

Action Fraud has not been terribly successful in pursuing—is happening through the use of bank accounts that theoretically should not be able to be used on the scale that they are.

We have a huge organisation, the Financial Conduct Authority, which seems to have the time and resources on hand at the moment to investigate all sorts of diversity quotas among its 50,000 members, but appears only to be able to muster 190 live investigations at the moment. For an organisation that regulates over 50,000 businesses employing millions of people, in which there are thousands and thousands of instances of fraud—it represents 40% of all crime in this country—the FCA does not seem to be doing its job very well, does it?

Baroness Vere of Norbiton: Unless you go into the detail of those investigations, I do not think you can say that. How can you say that?

Q484 **Tim Loughton:** Because, as I have just said, this is 40% of crime figures in this country at the moment.

Baroness Vere of Norbiton: How many retail banks are there that really have a volume of bank accounts in the country? There are not many. If those 141 investigations are focused on those people who provide the bank accounts, I suspect they are doing their job great.

Q485 **Tim Loughton:** It is 190 investigations. Who are they against?

Baroness Vere of Norbiton: I do not know, because we do not have operational control over the FCA. We do not do that. It is an independent regulator.

Q486 **Tim Loughton:** You have just said that the FCA regulates the financial sector, which has 50,000 firms. They are the firms that provide bank accounts.

Baroness Vere of Norbiton: No, that is not true.

Q487 **Tim Loughton:** Who else provides bank accounts that are not regulated by the FCA?

Baroness Vere of Norbiton: A group of them provide bank accounts. Not all of them provide bank accounts.

Q488 **Tim Loughton:** No, but just about everybody who provides bank accounts in the UK is covered by the FCA.

Baroness Vere of Norbiton: That is correct. The nine largest have to provide basic bank accounts, and they cover the vast majority of the market.

Q489 **Tim Loughton:** It is irrelevant, though. There are 190 live investigations. It might be that 189 of them are against one firm and one is against a smaller firm, or they may be against 190 different firms. That is not the point.

Baroness Vere of Norbiton: Therefore we do not know.

Q490 **Tim Loughton:** You do not know and I do not know. The point is that there are only 190 investigations going on and only 10 people have been prosecuted, and yet there are 50,000 firms where much more of this fraudulent activity, be it through the use of mules or whatever, is going on and it is not being traced. You have the FCA, with a budget of £780 million. Surely it should be doing more investigation. Where is that fraud happening otherwise?

Anna Harvey: A lot of those 50,000 firms are credit brokers; they are small lenders. The number of firms that have banking licences and are providing bank accounts is a small subset of that 50,000.

Q491 **Tim Loughton:** It does not just happen through banking accounts; it also happens through loans that are fraudulently engineered. Most of those regulated businesses have some capacity to be vehicles for various sorts of fraud. The surprise to this Committee was that the reach of the FCA, which is a large organisation, seems to be very limited in an area that is the largest single responsibility for crime in the UK, and where the use of bank accounts to facilitate that crime should not be happening, if it is fulfilling its money laundering obligations as it should be. Is that not a fair analysis?

Anna Harvey: It is a question that you rightly posed to the FCA. It is an independent regulator. We give it statutory objectives and it puts together a strategy for best pursuing those objectives. What it would have said to you is that its strategy is focused, given the large population, on supervision of institutions and on trying to ensure that the systems and processes that are in place across the system are robust. It uses individual prosecutions fairly sparingly because of the expense and the impact that it thinks that provides, compared with other areas.

Q492 **Tim Loughton:** It is an expense consideration that it only has 190 investigations.

Anna Harvey: It is an efficiency consideration.

Baroness Vere of Norbiton: Again, I do not see how you can say that 190 investigations is too many or too few unless you know substantially what those investigations are. It is impossible to draw that conclusion.

Q493 **Tim Loughton:** The more relevant statistic is that hundreds of thousands of fraudulent crimes are being committed each year. In a very substantial number of them, it involves the use of financial vehicles, which are offered by companies that are regulated by the FCA. It would appear that it is only analysing a very small fraction of fraudulent cases going through financial institutions. Otherwise, how do you explain it?

Baroness Vere of Norbiton: It depends on what the investigations are.

Chair: We have probably exhausted that, because you are saying that that is the problem that you have with being able to answer.

Q494 **Tim Loughton:** Are you happy that the FCA is an effective regulator and is doing everything that it is capable of doing to clamp down on financial fraud?

Baroness Vere of Norbiton: I am content that the FCA is an effective regulator. I have not heard people complain that it is not, but I would focus on what the FCA does to prevent fraud in the first place. For the FCA, it is much more about prevention and intervention along the process of fraud.

I absolutely accept your focus on bank accounts. I hope that the FCA took that message away and I hope that it is very clear about what it has to do for the big retail banks, but, as I say, it is an independent regulator. It is not under the direction of the Treasury. It reports to Parliament, and it is obviously accountable to Select Committees and so on. That is what Parliament itself decided that we would do for our financial regulators.

Q495 **Tim Loughton:** If the Government decided that the FCA was not doing its job properly, it is for the Government to bring forward regulations or legislation to change the way it operates—so it is independent, but it is ultimately marshalled and scrutinised not just by Parliament but by the sponsoring department, which is the Treasury.

Baroness Vere of Norbiton: We feel that it has the appropriate number of powers. There is no lack of powers here. It is a question of operationalising them.

I would also point out that, when it comes to money laundering, the FCA is one of 22 supervisors. Again, there are organisations that are not under the remit of the FCA that would be or could be involved in money laundering and terrorist financing. It is a very large ecosystem. The FCA does some of it, HMRC does some of it and then there are lots of others.

Q496 **Alison Thewliss:** How much money was raised by the economic crime levy?

Baroness Vere of Norbiton: It was about £80 million.

Q497 **Alison Thewliss:** So it is a shortfall.

Baroness Vere of Norbiton: Yes. When we introduced the economic crime levy, we said that we might have to make changes, because you can never quite know, when you introduce a new levy, exactly how much it is going to raise. There is a shortfall, and, as you know, we have now increased it in the last budget.

Q498 **Alison Thewliss:** You doubled it from £250,000 to £500,000.

Baroness Vere of Norbiton: Yes, only for the largest of businesses, with revenues over £1 billion.

Q499 **Alison Thewliss:** Did the Department get the sums wrong on how much you thought you would raise, or have companies tried to avoid paying into that levy?

Baroness Vere of Norbiton: No, it was just one of those things. We were absolutely clear when we introduced it that there might need to be changes made, depending on whether too much or too little was raised.

Q500 **Alison Thewliss:** How much do you expect to raise, given the increase?

Baroness Vere of Norbiton: We expect to raise about £110 million. We have slightly gone over, after the increase. We obviously need to make sure that it is fully funded.

Q501 **Alison Thewliss:** When will you know if you have made that money?

Baroness Vere of Norbiton: It will be after people have paid.

Q502 **Alison Thewliss:** I just wondered if you had a date in mind for when you were expecting to receive the funds for that levy.

Baroness Vere of Norbiton: No, because it is paid in arrears. We just put it up and it is paid in arrears.

Q503 **Alison Thewliss:** One of the concerns that we have heard from people throughout this inquiry is that the UK is not spending enough on tackling economic crime. The figure that I have is that the UK only spends 0.042% of GDP on tackling economic crime, and less than 1% of UK police resource is spent on tackling fraud. Is that enough?

Baroness Vere of Norbiton: I don't think it is about the money spent; I think it is about the outcomes. The economic crime plan is very much focused on outcomes, because one of the things that we are very clear about in the economic crime plan is that this is not just about Government; it can never be. That figure does not include what those in the private sector are using, all of their compliance departments and all of the structures that they have in place. It can never be just up to Government to fix this. I am content that we are spending an appropriate amount. It is actually a very ambitious plan—frankly, it is world-leading.

Q504 **Alison Thewliss:** There is significantly more economic crime being committed than the resource going towards it. If police forces are spending about 1% of police resource on a crime that is far larger than that, surely they are not going to be able to tackle economic crime.

Baroness Vere of Norbiton: I do not understand why you would make that connection.

Alison Thewliss: To me, the resources do not seem to be following the crime.

Tom Tugendhat: This is not just a policing operation, as you have rightly identified. The reality is that we are seeing policing interacting at certain points in this process.

The most important thing here is to prevent individuals from becoming victims. In many areas, that is where policing would be put forward—for example with public order, burglary or things like that—and having police on the streets may have a deterrent effect. This is one of those areas where it does not have that deterrent effect. It is actually about the investigatory effect.

You are looking at policing in a slightly different way here. That is why the important thing is not the raw numbers or the quantum of sums, but how policing works with business and with other intelligence capabilities. For example, the national fraud intelligence unit draws on the intelligence capabilities of the wider Government. The moneys from the NCSC or from GCHQ are not part of that figure; nor is the contribution made by Meta, HSBC or any number of other businesses.

I would argue that they are significantly more important, in many ways, than the raw number of police officers or the raw number of individuals being put on to fraud. It is only by looking at the whole thing together that you can see whether or not you are having the right effect.

Could we be doing more? Yes, but that is where a lot of international co-operation is so important. It is certainly true to say that we are beginning to have an effect already; that is the 13% decrease on the crime survey for England and Wales. I can only assume it is similar in Scotland. I am afraid I do not have the data for Scotland, for reasons due to different calculations, as you know very well. It is certainly true that we are seeing a greater effect.

Where do we need to put work in? We need to put work into co-operation with some of those countries that are not victim countries, but countries where perpetrators are based. We need to put work into making sure that a greater number of companies co-operate. That is why yesterday's summit was so important, and indeed why the online fraud charter is so important.

Q505 **Alison Thewliss:** The distinct impression that we have had from witnesses to this inquiry is that the police do not take this seriously at all, particularly when it comes to romance fraud. I will give you an example.

Anna Rowe, who set up the organisation LoveSaid, went to the police after being abused by a person on Tinder. She said they were very convincing and they were manipulative, but when she went to the police, they said, "So your boyfriend lied to you. What do you want us to do?" She did her own investigation and found 17 other victims of this fraud. Why are police not seeing this as a priority?

Tom Tugendhat: You are absolutely right that this is something that was not taken seriously and is increasingly being taken seriously. You are completely correct that, 10 to 15 years ago, people did not see this as serious at all. It has been growing in importance, and some police forces have seen it as more important at different points. That is why we are putting so much effort into this, because you are completely correct that romance fraud is nothing to do with romance. It is another form of swindling. It is just another form of fraud, and we need to treat it as criminal activity in the same way as we treat anything else.

You are completely correct in saying that all police forces need to treat it in the same way. That is why we launched the national fraud squad, which is now fully staffed at 400 officers. That is why we launched the national fraud intelligence unit under the fraud strategy, that is why we are leading on the online fraud charter, and that is why we are leading on the global fraud summit.

Romance fraud is not exclusively cross-border, but a large element of it is cross-border and very often includes countries where we would find it very hard to get a prosecution.

Q506 **Alison Thewliss:** Some of those people that committed frauds like that are still out there continuing to perpetrate these frauds.

Tom Tugendhat: They are, but very often they are in jurisdictions where we have no reach.

Q507 **Alison Thewliss:** Louise Baxter from trading standards spoke about this kind of online fraud as being organised crime, because it involves grooming, data sharing by criminals and bespoke targeting of people who are considered by the fraudsters to be vulnerable. Those people might not consider themselves vulnerable, so what more can be done to support those people?

Tom Tugendhat: This is one of those interesting phrases that I am slightly cautious of, because vulnerability suggests older people or people who may be—

Alison Thewliss: Louise Baxter talked about situational vulnerability.

Tom Tugendhat: You are exactly right. Forgive me: that is a much better term, because vulnerability can actually include a younger person who is very used to doing stuff online and is therefore much more trusting of an online process.

You mentioned Tinder. More young people use Tinder today than they did when I was at university, largely on the basis that it did not exist then. It is certainly a change in environment that causes that situational vulnerability that you have correctly highlighted. There has been a perception, which I am sure you would agree is an incorrect one, that fraud particularly affects older people, people living alone or whatever it is. That is simply not true. It affects everybody, and that situational vulnerability is really interesting.

This is where the work of the national fraud intelligence unit, alongside companies like Meta, is so important, because a lot of this is psychological. A lot of this is to do with the various different ways in which fraud happens. We have all received those emails promising us millions of pounds if we respond to whatever, and we assume they are a joke. They are not a joke. They are actually a way of fraudsters narrowing down their need to target individuals, because if you do not interact with them at all, that is easy: the fraudster has not wasted their time. If you do interact, you may be already demonstrating a level of credibility in something that is fraudulent that will enable them to decide that you are, as you rightly put it, a better situationally vulnerable target.

There is a huge amount of psychological work that needs to go into it, and that is why the intelligence lead is so important.

Q508 **Alison Thewliss:** Are all of the tech and social media companies taking enough responsibility, whether that is online dating, Facebook or Microsoft?

Tom Tugendhat: No, they are not.

Q509 **Alison Thewliss:** What needs to happen?

Tom Tugendhat: The reality is that some are. You will have seen the online fraud charter, and you will have seen who has signed up to it and how they have signed up to it. There are companies that have not signed up to it. We are having conversations with them.

Let us be clear: this is the first time that any country in the world has introduced an online fraud charter. It is the first time that any of these companies have signed up to recognise their responsibility for what is occurring on their platform. These are really big innovations and really big changes. It is therefore not entirely surprising that not everybody has signed up for it or that everybody is not at the same pace. There is more to do.

Q510 **Alison Thewliss:** Even for those that have signed up, it is voluntary. They could walk away and there would be no consequence.

Tom Tugendhat: They could. I would suggest that the reputational damage for doing so, now that they have accepted responsibility, is significantly greater.

Q511 **Alison Thewliss:** They do not seem terribly bothered about reputational damage. I have had representatives from Meta in front of Committees at various points. They did not acknowledge things like the TSB finding that a third of Facebook marketplace ads were fraudulent—they would not accept that.

Tom Tugendhat: This is where the conversations need to go further. Google is one company that has recognised its responsibility through the regulation. It has made sure that you cannot advertise any investment products that are not FCA-regulated on its UK platform. That has reduced what used to be about 20% of online fraud in the United Kingdom. Was it 20% of fraud or 20% of online fraud? It was 20% of online fraud, was it not? I will have to check the statistic, forgive me, but Google accounted for a large section of fraud in the United Kingdom. When it implemented that very simple rule, it went to zero.

That demonstrates that there is quite a lot that online tech companies could do if they chose to do it. You are absolutely right that this is where we need to be increasing the pressure, but there are reasons to be encouraged by the direction of travel, if not by the end state.

Q512 **Alison Thewliss:** There are regulations coming in the online safety field around paid-for content. If I put an advert on a social media platform, I am expected to comply. If I just user-generate content and put it out into the world and I am not paying for it, there is nothing that they can do about that.

Tom Tugendhat: You will appreciate this as well as I do. That is where the challenge of freedom of speech kicks in, because advertising a good is a different human interaction from having a conversation with somebody about an idea. I take your point.

The reality is that, yes, it is a different interaction, but it is right that as a Government we look at regulating those areas where paid-for content is clearly a business transaction rather than a human interaction, which is slightly different. Does that mean that there is a vulnerability? There is a vulnerability with all human interaction, but what we are doing here is taking the reasonable steps that are correct to take to keep people safe within the context of freedom of speech.

Q513 **Alison Thewliss:** On a slightly different note, do you think UK corporate structures are facilitating fraud? What can be done about that?

Tom Tugendhat: Not per se. If you are telling me that there are some fraudulent companies in the UK, of course there are. We are working to close them down, to fine them and to arrest those who are responsible, but not as a structure, no.

Q514 **Alison Thewliss:** I will give you an example. During covid there was a company in my constituency whose employees expected to get furlough payments. The company had set up a payroll company separately and had got the covid furlough payments, but the employees never saw any of that. That is a corporate structure set up to avoid responsibility to your employees.

Tom Tugendhat: I would argue that that is not only criminal, but incredibly irresponsible behaviour to individuals who were presumably extremely vulnerable to financial hardship at a time when the country was suffering. That is grossly immoral and deeply irresponsible.

Q515 **Alison Thewliss:** It is not uncommon to set up payroll companies to avoid obligations.

Tom Tugendhat: It is unusual to set up payroll companies to avoid obligations. It is normal to set up payroll companies to enable different financial and fiscal liabilities, but that is not the same thing.

Q516 **Alison Thewliss:** One concern that I have had for a long time is about the ways in which these corporate structures can be used to avoid the rules in place to protect people. I had it highlighted to me just this week that HMRC is still authorising a trust and company service provider whose only known clients are sanctioned Russians.

Baroness Vere of Norbiton: I will take that. If you want to send me details of that, I will certainly make sure that HMRC gets it, because everybody is very clear about who should be interacting with designated persons under the sanctions regime.

Can I just return quickly to the point that you made about the corporate structure? I am not entirely sure that the corporate structure is at fault here; it is people committing fraud.

Alison Thewliss: The structures allow people to do that.

Baroness Vere of Norbiton: Well, you can set up a company, but—

Q517 **Alison Thewliss:** There are companies and the people that are supposed to be the persons with significant control. All these rules that have been put in place are not being adhered to, which is allowing all this stuff to happen in the background.

Baroness Vere of Norbiton: Of course, and you will have seen the Companies House reforms that are coming in. I have an interesting stat here: six years ago, Companies House would have 10 investigations at any one time. It now has about 900 cases a month. Companies House is being resourced to be far more proactive.

Tom Tugendhat: We are also increasing that.

Baroness Vere of Norbiton: We are increasing it. They are being resourced to be far more proactive in terms of company structures. Under the ECCT Act there are reforms being done to Companies House, but in terms of the fundamental problem here, whoever set up that company was committing a fraud. HMRC spent £100 million on the taxpayer protection taskforce over a two-year period to recover, and it actually protected £1.6 billion by doing that.[1] I fundamentally agree that it is wrong.

Q518 **Alison Thewliss:** There is a new set of frauds being perpetrated against people. People are being registered as company directors without their knowledge or consent. What is happening to follow those kinds of crimes up as well? A researcher, Graham Barrow, has done a lot of work on this. People without any knowledge whatsoever have ended up being victims as a result, because it is not an obligation on Companies House to check these things.

Tom Tugendhat: That is where the Economic Crime and Corporate Transparency Act will kick in. It is the work that Kevin Hollinrake in the

[1] HMRC received a £100m investment for the two-year Taxpayer Protection Taskforce, and it recovered £693 million of the overall £1.6 billion HMRC protected on COVID-19 support schemes.

Department for Business and Trade has been leading on. You are absolutely right. There is the old story that Mickey Mouse was a director of I do not know how many companies. It is absolutely essential that Companies House is more than just simply a dumb register, a list of data or a data dump. That is what the ECCT Act does in order to prevent exactly that sort of offence. That is why we have empowered it. We have given it the ability to investigate and the resources to do so.

Q519 **Alison Thewliss:** It seems to me that the fraudsters and the enablers are always a few steps ahead of where Government are on this. That is why I asked Mr Ephgrave about the resources that Government Departments and agencies have to tackle this. It is difficult to recruit in the first place and keep those specialist staff when they can be snapped up by the private sector, and also by the fraudsters if they pay them enough money.

Tom Tugendhat: I would be cautious of going down that line, on the grounds that there are some people of very high integrity who are working in these areas.

Q520 **Alison Thewliss:** They are indeed, but in the past one of the police departments had talked about specialists on online fraud. They cannot keep them because they will go off to the private sector.

Tom Tugendhat: I come back to a point I made earlier: this is where the interaction between public, private and law enforcement is so important, because you are entirely right that organisations like Meta are likely to be able to pay more than Police Scotland or City of London police or whoever. It is also true that City of London police and Police Scotland or whoever have the ability to do things that a private company cannot. That investigatory capability is hugely interesting, it is hugely challenging, and it demands an awful lot of the individuals who pursue it. That, alongside the partnership in some of the technical skills that some of the companies offer, means that we can actually have a whole-of-society response, not just a Government response. That is really important.

You are absolutely right to focus on Government's responsibility in all of this. It is of course true that a Security Minister and the Treasury have responsibility—of course we do—but so does everybody. This is to Mr Loughton's point about banks issuing bank accounts, or to do with online.

Chair: We are straying slightly off topic, and I am conscious that Prime Minister's questions is in 15 minutes. Can you directly respond to the point that Alison was raising? You were rather drifting off into a broader picture.

Tom Tugendhat: My view is that this is a whole-of-society response, and Ms Thewliss has asked a very reasonable question on that. We all have a responsibility to play our part. It is certainly true that some offer more interesting career paths and some offer more lucrative career paths. Sometimes they overlap, but often they do not.

Q521 **Chair:** As we are very short on time, could you write to the Committee about the issue of 1% of police resources being used to deal with fraud? We are of the view that that is insufficient. We would welcome your consideration of that and what percentage it should be at.

Could you also let us know your view on the issue of social media platforms doing more to protect consumers from fraud occurring on their sites? That is particularly around this issue of reimbursing victims of advance push payment fraud, because we know that the majority of financial firms will have to do that.

Tom Tugendhat: Would you like me to write to you about this?

Chair: Yes, please.

Tom Tugendhat: I am very happy to.

Chair: Also, on your latest anti-fraud public awareness campaign, "Stop! Think Fraud", could you let us know what evaluation you are using to see what the effect of that campaign is? There are some issues with that. I would be very grateful if you could write to me with those three answers.

Tom Tugendhat: I am very happy to do that.

Chair: Thank you all very much for attending today. I hope you feel better very soon, Minister.

Tom Tugendhat: Thank you.