HOUSE OF COMMONS

Treasury Committee

Oral evidence: Economic crime, HC 145

Monday 14 June 2021

Ordered by the House of Commons to be published on 14 June 2021.

Watch the meeting

Members present: Mel Stride (Chair); Rushanara Ali; Harriett Baldwin; Anthony Browne; Dame Angela Eagle; Emma Hardy; Julie Marson; Siobhain McDonagh; Alison Thewliss.

Questions 95 - 198

Witnesses

I: Mark Steward, Director of Enforcement, Financial Conduct Authority, also representing the Office for Professional Body Anti-Money Laundering; Chris Hemsley, Managing Director, Payment Systems Regulator; Simon York, Director of the Fraud Investigation Service, HM Revenue & Customs; Martin Swain, Director for Strategy and Policy, Companies House.

Examination of Witnesses

Witnesses: Mark Steward, Chris Hemsley, Simon York and Martin Swain.

Q95 **Chair:** Good afternoon and welcome to the Treasury Committee and our inquiry into economic crime. We are going to be focusing this afternoon particularly on some of the key regulators, and I am very pleased to be joined by four witnesses. I am going to ask them introduce themselves briefly to the Committee.

Mark Steward: Mark Steward from the FCA. I am the executive director of enforcement and market oversight.

Chris Hemsley: I am Chris Hemsley. I am the managing director of the Payment Systems Regulator.

Simon York: Good afternoon. I am Simon York, director of the HM Revenue and Customs Fraud Investigation Service. That is the tax crime enforcement and anti-money laundering section of HMRC.

Martin Swain: Good afternoon. I am Martin Swain, executive director at Companies House with responsibility for strategy, policy and communications.

Q96 **Chair:** Welcome to all of you and thank you for giving us your time this afternoon.

For the first question, I am going to start with Mark and go to our other witnesses in turn. There has been a lot of press comment about a significant uptick in the level of economic crime that has been occurring since the pandemic started. Could you comment on that? In particular, if it is the case, what has the driver of that been and where have you seen the biggest increase in economic crime since the pandemic started?

Mark Steward: We would agree with the proposition that there has been an increase during the pandemic. The area where it is most noticeable for the FCA has been the increase in online scams and frauds. The particular focus for us is online advertising of regulated activities—those that we regulate—by firms that are not authorised by us. In many instances, we believe that some of those ads are scams and frauds.

The increase in these sorts of things started before the pandemic, but we noticed an immediate spike almost as soon as the first lockdown started. That was measured by us through the number of warnings that we issued. We detect these things online and then issue warnings to enable consumers to avoid these sites. The number of warnings that we issued, once the pandemic and the lockdowns started, really jumped quite markedly. In 2020, we issued just over 1,200 warnings, which was an increase of 100% on 2019. So far this calendar year, we have issued over 600. At that rate, it is an increase of more than 100% on last year, so there is a significant increase in these sites.

The increase in warnings is partially because we have changed the way we are detecting these things, in that we are more sensitive; none the less, it is a really dramatic increase. There are two main reasons why. We are spending more time online during the lockdown, which is noticeable to scammers and fraudsters, who are using that opportunity and exploiting reasonably loose controls around entry into the internet through social media. Social media does not have strong or robust means of detecting these things at the gateway, so it has allowed volume ads to be processed by social media, which are appearing in our searches on a daily basis.

Q97 **Chair:** Chris, what are you finding from your side of things?

Chris Hemsley: As the Committee will know, we have had a particular focus at the PSR on authorised push payment frauds or APP scams. In that respect, the year-on-year figures show that there has been an increase in terms of both number and value. The value has increased from around £456 million to £479 million. In terms of the types of frauds, it is very similar to the picture that Mark was talking about, with investment fraud and impersonation fraud being the larger items that are growing.

We track this on a more granular basis, and the most recent data that we have supports the idea that, during the pandemic, there has been this increase in fraud, particularly in the APP scam types of fraud. We did see a month-on-month increase in 2020, which is consistent with that view. It is quite difficult to be definitive, because there are a lot of other things going on.

In relation to your question about what is driving this, fraudsters are sophisticated criminals, so they adapt to any changes in vulnerabilities. While it is difficult to be too definitive from my perspective, the fact that a lot of us have been moving a lot of our lives online during the pandemic, using ways of paying and online banking—*[Inaudible]*—that is clearly—*[Inaudible.]* During the pandemic, we have all become more vulnerable. I am very conscious of the fact that some people—*[Inaudible]*—pressure on their lives to make them more vulnerable to these criminals.

Q98 **Chair:** You probably had just finished, but the quality of your audio was cracking up there, so I will leave that with you to have a quick thought about. Perhaps I could go to Simon for HMRC's point of view.

Simon York: In relation to fiscal fraud, we probably have not seen a huge change. Criminals found some of the things that we deal with a little more difficult at the height of lockdown—things like smuggling illicit goods or moving cash across borders—but we assessed that that was probably just a pause in activity, which picked up again as soon as things were easier.

The big change is in relation to some of the Covid support schemes, which did not exist prior to the pandemic. Those schemes now exist and are designed to pay out money, so they are naturally a target for criminals, as is any other scheme that pays out money. That is the change that we would see: probably not a great deal of tax fraud, but a new fraud that is there now.

Q99 **Chair:** Can I ask you specifically about bounce back loans? What is your assessment of the level of fraud that there might be within those loans?

Simon York: I am the wrong person to ask. HMRC does not administer bounce back loans and has had very little to do there. We support the banks with a verification process, where they can come and check against tax details, but we have not administered that scheme in any shape or form. We deal with the job retention and furlough stuff, "eat out to help out" and self-employed schemes. Those are the main ones we deal with.

Q100 **Chair:** Martin, give us the Companies House point of view.

Martin Swain: It builds on some of what Simon just said, but there has been some well-documented coverage of the use of UK corporate entities to continue to defraud. There was recent coverage around mini-umbrella companies being used. We are also working closely with colleagues in other Government Departments around some Government schemes, where, potentially, companies have been used as a vehicle to carry out illegal activity.

To put this into context, we are not an investigator in the same way some of the other regulators are, and we will probably come on to that in the meeting. In terms of our work with law enforcement agencies, just to give some context, we have dealt with 9,000 requests for information in the last year, which is up 50% on the previous year. That will give you an indication of the scale of work that we are doing.

Q101 **Chair:** Can I come back to Mark and ask about the banks? UK Finance is telling us that banks are doing a lot more nowadays to try to prevent fraud from happening. What is your assessment of how the banks are doing? What sort of changes or approach to regulation might you be looking at in this new terrain specifically as it refers to the banks?

Mark Steward: The evidence is that the banks are doing more; the question is whether they should be doing even more. There are things that they could be doing in addition. I mentioned our warning list, for example, which is the cornerstone of the strategy that we have to protect consumers. It was initially created specifically to help consumers, but it has now become such a key weapon that we also think that it should be used by banks, to ensure that they are looking very carefully at anyone on the warning list who might be a customer—so if they are banking anyone on our warning list—or who may be involved in paying out or receiving monies on behalf of anyone on our warning list.

Together with the assistance that we are providing to consumers, the warning list should be a key plank in any financial crime strategy particularly directed to things like authorised push payment fraud that has been mentioned in particular. We have recently published a financial crime guide as well, which should also be of value to banks and other financial services firms, including payment services firms, to ensure that their systems and controls are up to scratch so that they are not accidentally, let alone negligently, banking any proceeds of crime or money laundering.

While there is a lot that the banks are doing, it is something that they need to be constantly vigilant about. They also need to improve their systems and keep track of what we are doing, so that they can use the warning list to its best advantage.

Q102 **Chair:** What, if anything, is going on at the moment that is likely to lead to those improvements? Is there anything on the side of the system, the FCA or the banks?

Mark Steward: I will come back to the warning list. One big change in the last 12 months, in reaction to the increase in online fraud, is that we have sped up the process for issuing these warnings. Probably 15 months ago, we would detect these things through our surveillance work and then work out whether it was something we need to be pursuing from an enforcement perspective or immediately issuing a warning against. We knew that, if we issued the warning straightaway, our enforcement prospects were very low, because evidence would immediately go missing, if it existed. We would be tipping fraudsters off that we were aware of what they were doing.

The very significant increase in the numbers—and it really is a significant increase—has changed our judgment around that. It is now clear, given that we are going to be able to enforce against all very few of the things that we are detecting, the time taken to enforce and the cost of enforcement, that it is not really going to provide the protection that consumers need. We are now issuing warnings straightaway and conducting sweeps of the internet several times a day. We are issuing those warnings within 24 hours, so that they are up to date, providing valuable information to consumers about things they should be avoiding, and providing that same information to the banking system and payment services firms.

That is quite unique. I do not know of any other process like it anywhere in the world that is tackling online scams and frauds, particularly relating to investment scams and frauds. It is also quite unique because, traditionally, fraud was something that law enforcement could tackle only in an ex-post way. It was something that had already happened. People had already lost money. It was a long-running, difficult investigation, followed by a long-running, difficult prosecution.

Largely because fraud is a latent offence, it is not something that even the victims discover until they have realised that their money is gone, which can be some time after the fraud has been perpetrated. The difference with this online version is that it is happening, and we can detect it, in real time. The very thing that is creating the risk to consumers is also giving us the opportunity to attack it in real time as well.

The warning list is fantastic, and the way we are using it, hopefully, will start to reduce the incidence of these scams being effective. It may not stop them happening, because the production line into social media is a strong one, but hopefully it will allow banks to spot and report them to the NCA through the SARs regime or directly to us. It will also give consumers a heads-up about the things they should avoid investing in.

Q103 **Chair:** As you say, the warning list and acting quickly on it puts the fire out, but it does not grab the arsonist, if I could use that sort of analogy. Is there a risk with that approach that there are, therefore, people and criminal organisations out there that are getting away with it and left active, when they might otherwise not be, if you took a slightly more medium-term approach to catching up with them?

Mark Steward: While the warning list, in that sense, is designed to protect, inhibit and interrupt, it is not at the expense of the programme of pursuit or traditional enforcement, but it gives us time to look at the intelligence lying behind some of these sites and to identify some of the larger players, if we can. We can then spend time and money in going after them.

One of the really significant factors is that, in many cases, it is difficult to tell where these ads are coming from. Many have domains that are overseas. Many are using UK addresses and phone numbers that are not genuine. The address is not a genuine one, and the phone number is routed overseas. Identifying who is behind these scams—whether it is a small number of organised crime groups or a cottage industry—is something that we need to do.

We have many investigations on foot and we are working closely with other law enforcement partners in examining that very issue, but we have focused on ensuring that there is a protective shield in place to try to help consumers avoid becoming victims of scams in the first place. If we cannot immediately tackle social media sites because we have no power over them, we can do this in order to reduce the number of victims, and then tackle reducing the number of scams by tackling the perpetrators.

Q104 **Chair:** I have a final question for you, Chris, and could I ask for a fairly brief answer? Are the banks doing enough, and what more should they be doing at the moment?

Chris Hemsley: I would echo what Mark said: there have been a significant number of improvements, but there is always more to be done. There are some particularly tangible things, such as the completion of the rollout of confirmation of payee. This is the namechecking service, where we have got to around 90% of transactions, and we need to address the remaining 10%, where further systems changes are needed.

There are other opportunities in the information sharing space for making sure that we collate and then pass information to other firms, and particularly the recipient payment firms, so that they can act as quickly as possible on intelligence and flagged transactions.

The other part, which we will come on to talk about, no doubt, is that there is a lot more work to be done on protecting victims. We need to get that prevention piece in. That is really important, because prevention also stops people becoming victims in the first place, but there is more work to be done to make sure that those who do fall victim are then protected when they have done nothing wrong.

Q105 **Julie Marson:** Perhaps I could go back to Chris for a bit more detail about APP fraud and the contingent reimbursement model code. What are the pros and cons of the CRM code being made mandatory?

Chris Hemsley: The issue of making the code mandatory is something that I completely support. There are a number of significant benefits, the most obvious one being that you would be protected, regardless of whether your institution has chosen to opt into the code or to offer equivalent protection. That has to be a good thing. It is also good for competition, in making sure that there are minimum standards and that firms can compete on customer service in other aspects, rather than on whether they offer protection.

In terms of the downsides, I struggle to see that many. The real issue here is the way that we choose to do it. As long as the way that we choose to introduce this sort of mandatory protection is sufficiently flexible, so that it can adapt to how the criminals are adapting and so that we can learn lessons as we see what works. If we keep that flexibility, which is the sort of flexibility that is inherent in our regulatory framework anyway, that will allow us to make sure that we mitigate any risks and can learn those lessons. This is something that I support.

Q106 **Julie Marson:** When you talk about flexibility, I understand what you are saying. Recently, you said that the exceptions to the reimbursement obligation in the CRM code are open to interpretation. If there is some inconsistency in the code—and you talk about flexibility, which I can understand—does that endanger the consistency, when maybe we should be looking at more consistency under the code?

Chris Hemsley: I would distinguish between making sure that the rules are clearer and that people's compliance with those rules improves over time. My comments were particularly relating to that. As the code is

bedding in and people understand how to apply individual cases to the rules in place, there are still concerns that that job has not been done as accurately as possible, which is why the Financial Ombudsman Service plays a really important role in hearing those cases.

I would then distinguish that from the fact that those rules need to change over time. We might be able to improve some of those rules, based on experience, or we might find that those criminal tactics evolve in ways that we need to then reflect in new rules. I would make those distinctions. You need the flexibility to do the latter and to keep up with the criminals.

Q107 **Julie Marson:** You mentioned the FOS. How well placed and effective is it in ensuring that consistent approach to compensation?

Chris Hemsley: There are two bodies that are playing really important roles. The first is the Lending Standards Board, which manages the code. There is a series of reviews to try to learn lessons. It also checks whether banks and building societies are meeting their obligations under the code, so that is really important. The Financial Ombudsman Service then hears those individual complaints, where customers are not happy with how they have been dealt with. That is really important too.

The FOS is doing a good job in setting out case study evidence to try to improve people's understanding of how they see these cases. More of that to build understanding will help us to get all the banks and building societies up to the higher standard that we really want to see.

Q108 **Julie Marson:** Could you quantify some of this? We have seen roughly £479 million of APP fraud from 2020. How much has been repaid to consumers?

Chris Hemsley: In the latest year, it is just over £200 million. The year before, it was £116 million. Quite a few things are moving around here, but what we are seeing in the figures is that the introduction of that code meant that the reimbursement rate increased from around 25% or 26% up to 43% in the most recent figures. There is still quite a way to go, but, within a year, that is quite a significant step up and shows that the code is having a positive impact.

Q109 **Julie Marson:** You reported that less than 50%—a similar figure—of losses assessed under the CRM code are reimbursed. Is that good enough?

Chris Hemsley: The short answer is no. We published a document in February, where we looked through the evidence. One of the things we particularly focused on was looking at how that figure varies across different members of the code. It varies quite substantially, from around 30% up to maybe 75%. We cannot explain why there is such a difference in reimbursement rates, which then leads you to the conclusion that some members of the code are probably not fulfilling all their obligations. Again, that is consistent with the quite high rates of cases that the

Financial Ombudsman Service is seeing coming, and it is intervening in and overturning decisions quite significantly.

There is a long way to go, because we do not want it to go to the FOS. We want these issues to be addressed by banks, with their customers, without customers having to go through the stress, process and delay that the Financial Ombudsman Service inevitably brings.

Q110 **Julie Marson:** How are you addressing that inconsistency between banks?

Chris Hemsley: There are two principal things that are going on. One is that the Lending Standards Board has a series of reviews. It is expected to publish its latest update on Wednesday, in which it sets out information about how some of the exceptions to the code are applied and how it thinks members of the code are doing.

We also set out proposals in February to increase the level of transparency in this area. That is another tool that we have within the current legislation to explore how we can show which institutions are doing well at preventing fraud and protecting victims, and which really need to raise their game. There is a good case there for improving transparency as a way to increase performance.

As a final thought, in that conversation around transparency, we need to look beyond the code members, because they have at least signed up to the code. I know that other banks—notably TSB—have signed up to equivalent protections, but there are a whole number of institutions that have not, and we need to make sure that we paint an accurate picture across the whole market.

Q111 **Julie Marson:** That is very helpful, thank you. Just turning to Mark, the definition of vulnerable customers in the FCA guidelines is intentionally broad. Do those guidelines do enough to provide PSPs with a framework to identify and address vulnerable customers for APP fraud?

Mark Steward: We think that they do, and it is important for them to remain broad. If we were to be prescriptive, we would run a very real risk that we would leave someone out, because the categories of vulnerability are not really closed. It is a very firm belief on our part that all of us can be vulnerable in particular circumstances. None of us is immune from becoming vulnerable as well.

We have tried to think through how you can create a better definition that might be easier to apply, but, in reality, it is the sort of thing that we should all be able to recognise. We would expect the firms that we authorise to recognise it as well, given the overlay of other obligations that they have, including the need to treat customers fairly. It is an inevitability of ensuring that no one is left out that we have a broad enough definition to capture everyone.

Q112 **Julie Marson:** Perhaps I could turn to Martin for a Companies House

perspective and talk about transparency and company formation. We have previously reported the risks from company formation, and we saw that in FinCEN files as well. The cost is £12 in the UK and, in Europe, the average cost is about €800. Would increasing formation costs reduce the attractiveness for money launderers forming UK companies? Would it also raise money to fight economic crime?

Martin Swain: I will deal with the final part of the question first. In terms of increasing the fee, it is probably worth the Committee being aware that we operate on a cost recovery basis. Legally, we can only recover the costs that we are directly creating for the customer. The interesting thing about the incorporation fee is that, the more efficient we become, the more digital we become and the more we drive down the cost. That is one aspect to this.

I guess the question would be to what level you raise it where it becomes a disincentive for a criminal, be they a low-level criminal or someone involved in serious organised crime, to use the UK system for that abuse. I would not be able to put a figure on it. I would make the assumption that, if an organised criminal gang wanted to use a corporate entity for abuse, even if we had the same fee as some European registers, it would not disincentivise it that much.

Hopefully, when we get the legislative reform, the things that we put in place will be a bigger disincentive for people who are engaged in criminal activity. We believe that verifying identity will be an immediate disincentive for people to try to create a company for illegal purposes. Our view at Companies House is probably that the fee is not the main driver.

Q113 **Julie Marson:** Is that why the consultation by BEIS has been looking at the whole package of company formation rather than the cost, which has been excluded?

Martin Swain: Yes. The reforms that the Department has set out are the biggest ones to Companies House since it was formed in 1844, so the scale is huge. We are hugely supportive of the Department's position on this, to the point that it frustrates us, an agency, that we cannot act more proactively in this space. The suite of measures in reform will give us much more of an impact than if we just raised the fee for incorporation.

Q114 **Julie Marson:** Can you give us a sense of the progress of the project, where we are and when it might go live?

Martin Swain: It is probably more a question for Ministers on the timing of the legislation. We in Companies House are chomping at the bit to get on with reform. We are in year two of a major transformation programme, where we are upgrading our systems, developing the capabilities, and putting in place the kind of infrastructure that we need to deliver on the reform. We are getting ready, but, ultimately, the legislation switches much of this on.

I suppose I should say that, in terms of economic crime, we are trying to exploit as much as possible our current powers or where there may be powers in other legislation that we can use with partner agencies to contribute to tackling economic crime. Simon will be aware that we did some partnership work with HMRC under the Digital Economy Act, for example, where we identified companies that were fraudulently filing a set of accounts with us and a different set with HMRC in order to avoid tax. We are trying to do as much as we can within the powers that we have but, as the reform consultation makes clear, there are lots of limitations to our current powers.

Q115 **Julie Marson:** We might be speaking to Ministers about this, but what elements of legislation are you most keen to get on with and see implemented?

Martin Swain: The package as a whole is really important, because they fit together. ID verification is one of the key aspects of the reform agenda for us. Knowing who is setting up and running a company, and transacting on their behalf, is hugely important, not just from a transparency perspective. From a prosecution perspective, it is hugely important for us to understand who it is who has committed an offence, so that we can pursue them.

There is an awful lot of the reform agenda that talks to the accuracy of the register, which is a hugely important aspect for us in Companies House, so that individuals, consumers and businesses can have trust and confidence in the data that we hold. We would be the first to admit that, in many areas, we have difficulties in ensuring that accuracy, again because the current legislation requires people to submit complete information. If it is complete, we are legally required to register it. Even though, sometimes, we know that the information is incorrect or potentially fraudulent, the registrar is legally required to register, so accuracy is hugely important.

Probably the final main plank is around protecting personal information, so that we do understand the importance, when we hold information, of protecting individuals from harm. If we are verifying ID in the future, we are potentially going to be holding even more personal information, so having things in place that protect that information is really important for us.

Q116 **Julie Marson:** Is part of the problem company formation agents?

Martin Swain: It has been fairly well documented that, in many instances, agents are the cause of an issue. If I take ID verification, for example, we will not just require directors and PSCs to be verified, but if an agent is acting on behalf of the company we will want to verify the identity of the agent themselves and that they are properly supervised, which we do not do at the moment. Anybody can file information on behalf of a company and we do not check who they are, so that is hugely important. There is wider work in relation to formation agents and TCSPs,

and we are plugged into that work from a Companies House perspective so that we can work with our partners on that. It is a really important issue for us.

Q117 **Julie Marson:** Is it still the case that you have not imposed any fines or prison sentences around beneficial ownership information?

Martin Swain: If the Chair would want me to, I can provide some detailed statistics afterwards, but we do take prosecutions forward for PSC offences. In the last few years, we have done just over 300 prosecutions for PSC offences in England and Wales. In Scotland, we are a little behind, and I know that Alison has been interested in this in the past, but we are now working with the procurator's office and, at the moment, have 50 live cases in the system. We aim to put about five referrals a week through in Scotland, so we are building it up, but we are a bit behind there. We are taking action and it is not always easy. Again, it goes back to the issue of the natural person. If you do not have the natural person, it is very difficult to go after the prosecution, but we are very active in that space now.

Q118 **Julie Marson:** I have a final question for Mark. What action has the FCA taken following the revelations in the FinCEN papers? Banks still seem to be able to move money for suspicious clients and the UK is still deemed to be high risk. What is the FCA doing about that?

Mark Steward: We have a very significant programme to tackle a lack of money laundering systems and controls by firms that we regulate. Some of the largest fines that we have imposed have been against banks for systems and controls failures. We have recently commenced the first criminal prosecution under the money laundering regulations against a UK bank in relation to the same matter. It is probably one of the most significant parts of our enforcement programme.

The FinCEN allegations largely constituted things that were already known by us. They were historical and had been the subject of action either here or in the US, where many of the matters really related. The important point to make in response to your question is that we have an ongoing, continuous programme of supervision and enforcement relating to money laundering controls and systems.

Q119 **Rushanara Ali:** I am going to focus my questions on the Online Safety Bill and consumer investment fraud. As you were responding to the Chair's questions, I was thinking about a telephone call that I got earlier today, telling me that my national insurance number had been compromised and that I should call a number and press a button, to the effect of giving more personal data over. In the past, the NCA has been invoked in calls like that, and I certainly know of constituents who have rung up and been very anxious. Sometimes, people end up easily being led into giving information, so the point is well made about anyone being susceptible or targeted. What we see now is more and more social media platforms pushing adverts.

Mr Steward, the Online Safety Bill is a really important opportunity to address some of the challenges. The former head of the FCA and now Governor of the Bank of England has mentioned this at times, not least the LCF case. When he came and gave evidence, he referred to it. The current FCA head has referred to this as an opportunity. Should the Online Safety Bill require search engines and social media platforms to implement a level of due diligence on the advertisers that use their platforms to prevent scammers promoting fraud? That is not included in the draft Bill.

Mark Steward: First, we are very pleased to see the inclusion of fraud in the Bill. That is a very big step forward, because it was not in the original draft of the Bill. We are concerned about the breadth and scope of what is currently in the Bill, because it is a bit unclear from its wording, but it does look as though some content that is at the heart of the problem we are trying to address would not be covered by the way that the Bill is currently framed. We are very interested to see how that will pan out through the Bill's scrutiny process.

Q120 **Rushanara Ali:** Yes, but it should be.

Mark Steward: Yes, of course. It should be clearly included; otherwise, there is no mechanism for social media to be legally obligated to do some very basic things that do not happen now, such as ensuring that the person who is placing the ad is someone they know, they know where the person is, and they know that the address and contact details are correct, or, where the person is advertising a financial investment, that that firm is properly authorised by the FCA to do so. At the moment, those checks are not being made, and there is no legal obligation either.

Q121 **Rushanara Ali:** Have you had any feedback from officials and Ministers on taking this point on board and making the necessary changes to this important Bill?

Mark Steward: We are very conscious that there will be a Bill scrutiny Committee process in relation to this particular Bill.

Q122 **Rushanara Ali:** I am aware of the scrutiny process. I just want to know if the FCA is getting the appropriate receptiveness to this particular provision, so that we get it into the provision, rather than having to rely on Back-Bench MPs having to put amendments in to try to persuade the Government to make the necessary changes that you think would be helpful.

Mark Steward: We have made our position very clear through a number of fora, and I have made speeches about this in the last few weeks as well, which have been published, saying that this is something that we would like to see.

Q123 **Rushanara Ali:** Have you had the dialogue with Ministers and officials that gives you confidence that they will take on board what you are talking about?

Mark Steward: We have not done that yet, but we are very happy to. Our public position is very clear.

Q124 **Rushanara Ali:** The FCA is paying Google £600,000 a year to post scam warnings. Is it appropriate for a regulator to have to post warnings while Google profits from social media companies that make money out of fraud, or should you be empowered to make it do that without you having to waste money?

Mark Steward: We would prefer that these ads were not published in the first place, to be really frank. The irony of us having to pay social media to publish warnings about advertising that they are receiving money from is not lost on us.

Q125 **Rushanara Ali:** Are there any other companies that you are paying, as you are Google, to do this?

Mark Steward: We run several very expensive, for us, ScamSmart campaigns, which is our way of educating consumers about the sorts of scams we are seeing, the sorts of things that consumers can do to avoid being scammed in the first place, and what to do if you get the text message or the phone call saying that you are under the investigation by the NCA or that someone has your national insurance number, whatever it might be. We tell people what to do. We run social media, television, radio and newspaper advertising. We pay for all of that.

Q126 **Rushanara Ali:** It does make a mockery of the regulator that it has to pay companies that continue to profit from fraud. Is it not obvious that the Government should stop putting the regulator in a position where, frankly, Google and the like are laughing their way to making double amounts of profits: first from fraudulent sites being hosted; and, secondly, by extracting money from you as a regulator to take them off and give warnings?

Mark Steward: As I said out the outset, we would prefer that these ads were not being published in the first place. We have been in discussions with Google, which has offered us a credit in relation to these expenses in the future, which we are in the process of considering at the moment.

Q127 **Rushanara Ali:** Has it confirmed that it will give you back that £600,000 a year?

Mark Steward: I am not sure that it has gone that far.

Q128 **Rushanara Ali:** It ought to. It is profiting from fraud and costing the Financial Conduct Authority money. I would be really interested to know what happens with that discussion, whether you are going to get your money back and whether it can give you an undertaking that this is not going to happen going forward.

On the numbers, we have already heard about the total number of reported incidents of investment scams quadrupling between July and October 2020, from 300 to 1,175, and the average cost of fraud being to

the value of £46,000. Chris Hemsley, what action is being taken to prevent investment fraud by other payment systems and the cloning of websites of reputable investment firms? That is another one that is very easy for any one of us to get entrapped into doing, never mind more vulnerable or less savvy customers.

Chris Hemsley: Where the PSR fits into this is particularly in closing off some of the vulnerabilities around impersonation for the initial payment. That is this namechecking service, confirmation of payee. A tactic that is part of these frauds is that they encourage you to make a transfer to a fraudster, when the name that you are typing into your internet banking platform is a legitimate business. Confirmation of payee focuses particularly on that.

The wider issues of regulating and supervising investment fraud are principally for Mark, as he has been talking through, but we are playing our role in making sure that, where we can, we make it harder for criminals to conduct these frauds.

Q129 **Rushanara Ali:** Mark, did you want to add anything to that particular issue about the cloning of sites?

Mark Steward: One of the biggest increases in the online scams has been the use of clones of FCA-authorised firms. We see this as a direct response by scammers of some of the warnings we have put out and the advice we have given to consumers to rely upon the FCA register as a safe place. To get around that advice, scammers have started to use the FCA register and clone the names of those firms. We conducted a substantial ScamSmart campaign earlier this year and amended our advice on our ScamSmart website to help consumers avoid falling for a clone, and to ensure that they were dealing with a legitimate FCA-authorised firm.

This shows that the work we are doing, including our work on consumer protection, ScamSmart and the warnings list, is the genuine front line against scammers. Whatever we do, they are trying to respond to it, and this is an evolving picture all the time. I mentioned earlier that we want banks and payment services firms to continue evolving their own approaches, as we need to as well, because some of the best entrepreneurs out there are scammers. They are using different tactics all the time to get around the advice that we are giving consumers. This is a gripping story and it is really important that we can put money into things like ScamSmart, because it is an incredibly important public service.

Q130 **Rushanara Ali:** I get that, but there is a responsibility on online companies for knowing those who are on the platform and carrying out fraudulent activities, and for knowing their customers, as you would expect from banks, for instance, and other providers. As Graeme Biggar from the National Economic Crime Centre said to this Committee, "They should know who they are dealing with. They should remove fraudulent

sites. They should report to law enforcement on the fraudulent sites."

I have noticed that more adverts are coming through on platforms like Twitter and search engines like Google. Is it not time for a seismic shift in terms of social media companies having responsibility for companies that are clearly engaged in fraud, so that they are the first line of the frontier? Otherwise, it is costing taxpayers, because you or other agencies are paying for it. Ultimately, you are putting plasters on the wound, if online companies do not take action in terms of knowing their clients who are using their platforms to carry out fraudulent activity.

Mark Steward: We agree completely and we are engaging with all the social media companies and making it very clear that we expect them, even now, without the Online Harms Bill being enacted or perhaps applying as broadly as we just discussed, to be taking action to reduce the number of scams that we find on their sites.

Chris Hemsley: I completely agree with Mark and support that effort. We want all parties to play their role, and that includes social media firms and other communications firms that are introducing vulnerabilities and costs into the system, which are then ultimately borne by the financial services sector and customers. I completely support what Mark just said.

Q131 **Siobhain McDonagh:** Rushanara has covered most of the aspects that I wanted to ask. It is all very well to say, "The Facebooks and the Googles should," but they are enormously powerful companies, and the FCA is just a regulator in the UK. What are these companies like to deal with? Do they take much notice of you? Will they act when you ask them? Do they take any responsibility themselves? What is your relationship like with them and what challenges have you experienced with them?

Mark Steward: We have good engagement from the social media companies that we have been dealing with. In many respects, the problem we have described is one that is shocking for them as well. The challenge is whether they are really able to come up with a way of tackling this problem that is also consistent with their current business models. In many ways, consumers and advertisers having ready access to what is on the internet, being able to find ads that are tailored to their needs, and being able to see YouTube programmes, Twitter feeds or whatever it might be that answers their desire or demand, means that the gateways are naturally very low. They function best when those gateways are open and can allow volume through.

What we are requiring them to think about is how that can be interrupted by some kind of programme that identifies the very things that are going to cause damage to consumers. It is fundamentally important that something like that happens, but there are some logistical challenges as well, some of which we are discussing with each of the firms that are involved. We shall see how successful they really are, because the proof will be in the pudding. If the proof is not in the pudding, we are going to have to take action of a different kind.

Q132 **Siobhain McDonagh:** What history of success is there of voluntary actions by the Google, the Facebooks and the Twitters? At the other end of the spectrum, I am more aware of the scams that are carried out against children and young people in my constituency, who are used as money mules. It affects them long into the future. These companies promise big and deliver small. What are they doing and what effectiveness have you seen?

Mark Steward: At the moment, the ball is in their court, so we shall see what they come back with. The phenomenon we have described has occurred over the last 12 months. You have heard about the steps we have been taken to try to address it; that is our way of tackling it as quickly as we can. The next step, which is evolving a longer-term solution with the social media industry, is really important now and is where we are right now.

Q133 **Anthony Browne:** I have some questions about gaps in powers that the FCA and the PSR have in particular. I just want to follow up Siobhain's and Rushanara's questioning. Like most people, I am absolutely shocked at the fact that social media companies, Google in particular, profit from promoting fraud. The legal definition of fraud is "gaining financial advantage by deception", and Google is gaining financial advantage here and deceiving its customers. It is not the generating of content that is fraudulent, but the ones that put the fraudulent content out there and enact the deception.

It seems to me that there is a legal case to be made here. I am not a lawyer, but I have been involved with quite a lot of actions against fraud, particularly when I was chief execute of the British Bankers' Association. There is a prima facie case here that you could say that Google is guilty of fraud. Mark, I am interested in your views on that, and then I have a follow-up question.

Mark Steward: I am not sure that I am going to comment on the strengths or weaknesses of the prima facie case, but I will say that there is a provision in the Financial Services and Markets Act that means that particular financial promotions can be communicated only by a person who is authorised by the FCA, or the communication must be approved by a person authorised by the FCA. The 1,200 warnings that we issued last year, which we saw on Google searches, were not for advertisements that were issued or approved by any FCA-authorised firm. This is something that Google could have recognised at the gateway, before allowing that ad to appear on its searches, but it did not have any mechanism for identifying what is and is not a financial promotion that requires this treatment.

Further, there was an exception to the rule in the UK that disapplied this obligation for advertising that was sourced from an EEA state. This exception applied right up until 31 December 2020. Since we left the EU, this exception does not apply, so the rule under the Financial Services and Markets Act that requires financial promotions to be issued or

approved by an FCA-authorised firm applies to social media companies, as it does to all media companies and anyone who is communicating a financial promotion. That is the issue that is squarely before social media right now: can they comply with this provision or not? If they cannot comply, we are going to have to do something about it in a more formal way.

Anthony Browne: You are suggesting there that they are breaking the law in terms of FSMA.

Mark Steward: The law changed on 1 January this year and it is not immediately apparent whether social media was really aware of what this change meant. We have made them aware and we now have quite a lot of traction with the social media industry to force change or to see change. If not, we will take action.

Anthony Browne: You are hinting there that you will take legal action against social media companies such as Google, if they do not comply with the Financial Services and Markets Act.

Mark Steward: Yes.

Q134 **Anthony Browne:** I urge you not to be wowed by the social media companies saying that their business models require this, that they have to do it at volume, and that it is all very difficult from a logistics point of view. They are the biggest and richest companies in the world. They show that they can do almost whatever they like, and it is a question of will within the company. While they are carrying on making profit out of fraud, they have very little internal incentive to minimise that.

They have reputational issues, but one of the things we know about social media companies, even when they employ former Deputy Prime Ministers of Britain, is that they are incredibly good at not reading the public mood and public opinion, and are always behind the curve on this. Certainly from my point of view, I would urge you to take very strong legal action against them and treat them as you would treat any other company. Do not cut them any slack if they say it is very difficult because of their business model.

On the point of whether Google itself is guilty of fraud or gaining financial advantage from what it is doing by deceiving its users, you do not want to comment on the prima facie case, but you have a lot of lawyers at the FCA who specialise in fraud. Could I ask that they look at whether Google is corporately guilty of fraud by profiting from promoting fraud against citizens in the UK? Can you confirm that you will do that and then supply that opinion to the Committee?

Mark Steward: We will comply to the best of our ability.

Q135 **Anthony Browne:** I will accept that, thank you.

The other questions I wanted to ask were about gaps in your powers. You probably do have enough powers on what we were talking about, but the

Government recently launched a consultation on the power to block listings on national security grounds. That is not a ground that you currently have. You control the rules around listings otherwise. Is there a need for such a power and will it make a difference, or is it so outside of your scope that you have not thought about it?

Mark Steward: It is certainly outside the FCA's scope. We are not the guardian of the national security interests of the United Kingdom. If there was a listing that threatened the national security interests of the United Kingdom, we would not be the ones to spot it. Someone else would have to spot it and provide us with the right guidance at that point.

Q136 **Anthony Browne:** This suggested power applies only for the main official list on the stock exchange, not for junior markets such as AIM. Would that be a gap?

Mark Steward: Having been professionally thinking like a scammer, I can only think that, if there is a loophole, it will be exploited.

Q137 **Anthony Browne:** That is a fair assumption. As you said, scammers are some of the best entrepreneurs in the country.

Coming to Chris now and the Payment Systems Regulator, I understand that the PSR was not mentioned in the Government's 2019 economic crime plan and that you lack the appropriate powers to take action against the use of payments infrastructure for economic crime. I declare an interest as former chief executive of the British Bankers' Association and used to be heavily involved with its predecessor organisations. Pay.UK, which is an industry body, was given responsibility for creating a new payments architecture in the economic crime plan, but it is an industry body that is fundamentally industry-led. Should the PSR have more powers to tackle economic crime?

Chris Hemsley: You are right that Pay.UK, given its ownership of the infrastructure and its role, is the right body to be a direct participant in that plan. Our role as its regulator is to make sure that it discharges that role and protects users.

In terms of our powers, we have highlighted that there is a current barrier in UK legislation that prevents the PSR using the powers that we have more generally to address this issue of making reimbursement mandatory. We currently have a voluntary code, and one of the reasons why we have that rather than a mandatory regime for protection is that there is this limit on our powers. That limit originates from a piece of European legislation. In a similar way as Mark was just talking about, there was a period when it was much more difficult to address that legislative barrier to the PSR acting, but there is now an opportunity, following withdrawal from the European Union, to address that issue with legislation, which is in UK law.

We are working with officials to understand the opportunity for making that change, so that we can, where appropriate, take that action and

move from this voluntary approach to considering using our powers to move to a mandatory protection regime.

Q138 **Anthony Browne:** Can you describe how a mandatory protection regime might work? Would set down in law the circumstances in which, where you have payment fraud of one type or another, banks would have to make repayments for the fraud?

Chris Hemsley: It could work in a number of ways. You could have quite a lot of detail in the primary legislation. We thought about this and, in February, set out our ideas around how this could work. It made particular use of the scheme rules. The payment systems have rules around data sharing, information and how the systems work, and there is a good case that interbank rules—things like faster payments—should include minimum standards of protection for consumers.

There is a difficulty around having clear enough rules that you can codify to then being sufficiently flexible to deal with fraud as it evolves over time. One of the proposals that we set out was to include a requirement to be a member of an approved code. We have one code at the moment. That would allow the approved code to evolve over time. That is a particular way that you could reconcile those competing pressures between the need for clear rules that go into systems and into legislation, and the need for flexibility over time.

Q139 **Anthony Browne:** I have a follow-up question for Mark Steward. You talked earlier about the rules on compensating consumers who are victims of fraud. What do you see as the responsibility of consumers in this? One of the points that financial services companies often make is that they also have a responsibility to guard against fraud. If you always compensate everyone who is a victim of fraud, you remove any incentive for diligence.

One example that is often given is if you give somebody your bank card with your PIN written on it. If you hand it to a stranger, you should not be surprised if money leaves your account. In that case, the bank would rightly hold the customer responsible for what is, in effect, fraud. In other circumstances, if you have your bank card stolen and it is used in another way, you are not responsible. What are the responsibilities of consumers?

Mark Steward: The obligation that we have is to ensure reasonable protection for consumers. In the legislation that we administer, the protection to consumers is not absolute, but there are some challenges here around what the limits of protection really can be in practice. You quoted earlier a definition of fraud involving obtaining financial advantage by deception. Dishonesty is an important part of fraud. Someone being deceived is an important element of fraud. Any of us can be deceived. Even highly sophisticated businesspeople can be deceived by fraud, and it is in the nature of fraud that it can often be enormously sophisticated and cunning, and can exploit all the defences that we all think we have.

Some of the research we have conducted is to the effect that many of us think that we can spot a fraud, so we feel invulnerable, when, in fact, our very confidence is what makes us vulnerable. It is a bit like watching a magician. You see the simplest of tricks, and yet you cannot work out how it is being done. All of us can be made vulnerable.

In those circumstances, I have no doubt that a victim should be compensated. The primary compensator, of course, should be the fraudster. We are in court today seeking confiscation orders against four people who have been convicted of fraud offences in prosecutions that we have brought, in order to try to do that very thing. We have proceeds of crime restraint actions on foot in nearly 30 cases, where we have frozen money that we believe might be the proceeds of crime, for the very purpose of ensuring that, if we get convictions, we can return that money to the victims.

The system needs to work in a way that does not create too many obstacles for victims of fraud when they are victims. At the same time, the system needs to ensure that it is prepared to be accountable when it has failed those consumers and perhaps facilitated the fraud that has occurred.

There are various other harms that can occur to a consumer and, of course, there are many things that consumers should be doing to protect themselves, including looking at the information we place on our ScamSmart website, which is full of really valuable information for all consumers to avoid becoming a victim in the first place, and using our warning list.

Q140 **Anthony Browne:** Can I ask you about a real-world example that I got involved with when I ran the British Bankers' Association? Vince Cable came to me with an example of a constituent of his who was buying a house. Some fraudsters had intercepted the lawyer's email and said, "Can you transfer the money into this account rather than that account?" So they instructed the bank to transfer the money into the new account. The bank said, "Do not pay money to that account. It seems to be associated with fraud."

The customer came back and said no, and gave an instruction to the bank to transfer the money into the account that the bank had told them not to transfer it into. They said, "We are the customer. We are buying the house. Do not mess up our house purchase". Sure enough, they lost their money, which is tragic from the consumer's point of view, but is the responsibility there with the bank to refund the house purchaser, when it had tried to stop the consumer doing it? Ultimately, it is the consumer's money and they have the right to instruct the bank to do what they want with it.

Mark Steward: The bank is obliged to act on that instruction as well. I learned a long time ago not to give off-the-cuff opinions, so I do not want to give one. In that example, the one thing that I would say is that,

where the bank is saying to the customer, "Do you really want to do this? Do you really want us to transfer that money?" it is probably important for the bank to explain why it has misgivings about the transaction; otherwise, the customer is not really getting the full picture.

I would like to think that a bank acting in the best interests of its customer, or in a way that is designed to proceed a fair outcome for the customer, would tell a customer what information it has that is making the bank itself concerned about the validity or the legitimacy of that transaction.

Anthony Browne: I totally agree with that. I know that there is a lot more that the banks could do on that.

Q141 **Alison Thewliss:** I have some questions around enforcement action on money laundering. Simon York, the economic crime plan requires HMRC to conduct an annual self-assessment of money laundering supervision. The latest report was published on 17 March this year and found that you were meeting your obligations under the regulations. Is this just a case of you marking your own homework?

Simon York: No, not at all. This was a commitment that we made as part of the Government's economic crime plan that we would work to the standards set by OPBAS and, as part of that, carry out a self-assessment each year to check that. We carried out the first one of those and involved OPBAS in that process, and the Treasury signed off the final document. It was a thorough investigation. I have read through the whole thing and it was conducted by someone independent from this area of business within HMRC.

Q142 **Alison Thewliss:** But they were not really independent from HMRC altogether. Would it not be better to have somebody external look at this?

Simon York: We have had external people look at it to a degree. FATF came to the UK in 2018, and the UK got a pretty good assessment then of its supervisory activity and HMRC's part in that. We are starting from a fairly strong foundation in terms of external assessment of our ability as a supervisor, but we have put a lot of work into that since that point. We have worked through all the action points that we committed to in the economic crime plan and have made a lot of progress. I can talk to you about some of that if you wish.

Q143 **Alison Thewliss:** I would like to ask a bit more about company formation agents, which is something that this Committee had asked for more work on and is not referred to in the self-assessment. Can you give a specific update on what you have been doing around company formation agents? To me and many others looking at this, those would be seem to be the biggest gap at the moment.

Simon York: To set the scene a little, HMRC supervises about 33,000 businesses across nine sectors, of which trust and company service

providers are one. It is worth noting, though, that we supervise only about 6% of that market. The rest of trust and company service providers are supervised either by professional bodies like accountants and lawyers, or the FCA or whoever. So it is one of the sectors we supervise. We recognise that they can be high risk given the role that they play in creating companies. We heard earlier from Companies House, and we would absolutely agree with that. We see the creation of companies as a significant issue when dealing with tax crime. It is a significant part of organised criminals' MOs in that.

We are aware of that being a risk, and have invested quite a lot recently in improving our understanding of this sector and the risks in it. We have done work with partners from across Government and the private sector on that. We have been running targeted campaigns on higher-risk sectors. Within this sector, the highest-risk bits are those businesses that offer multiple services or virtual office services, and those that are not on our register in the first place. We have run a series of campaigns aimed at those high-risk areas. For example, we ran a big campaign around a company formation agent that was using a lot of Scottish limited partnerships. We have also done something recently around virtual offices.

We also put a lot of energy into educating the people in this sector. We find that most of these businesses react well when we highlight their failures and the common issues that they could avoid. In terms of what is coming up, we have a significant period of action planned for a little later this year, which will have a real variety of activity. Some of it is going to be educational, with a series of webinars alongside the NCA, talking to people about fraud and SARs. There is going to be a real push on unregistered businesses and looking at those people who are advertising this type of service, but who are not yet on the register. We are also going to be targeting the highest-risk TCSPs for compliance inspections and enforcement activity. We recognise that this is a high-risk sector that needs more doing with it, and we are on with that now.

Q144 **Alison Thewliss:** It seems all very well to have campaigns, to advertise what you are doing and to warn people, but the *Ferret* has found that there are 797 companies registered at one address at 12 South Bridge in Edinburgh. Bellingcat has found that 91% of SLPs are registered at 28 addresses, and there are significant numbers of these. Why are you not doing more about that?

Simon York: That is definitely an issue that we are aware of. Without talking about any individual businesses or situations, whenever those reports are made or whenever we get intelligence provided to us from a range of perspectives, we do something about those things, if they are within our supervised population, which they are not always. If there is something amiss, we absolutely would tackle those sorts of things. We recognise this from our tax crime work. We are the victim of this as well in terms of the creation of multiple companies. We see that as a way of

organised criminals attacking the UK tax system, so we are very alive to all of that. HMRC has a particular advantage in this space in the sense that we are not only the supervisor of these businesses, but we are also the UK's tax authority and we deal with their tax affairs. We are also a full enforcement agency, so we have the same powers as the NCA or the Met Police. We are significantly active in this economic crime and anti-money laundering space.

Q145 **Alison Thewliss:** I would suggest that these companies are not interested in your campaigns or in complying; they are interested in moving money around in the best way that they can, without you finding out about it. Maybe I can bring in Martin Swain from Companies House to take his perspective on this.

Martin Swain: This goes back to the question of reform and the powers that that will give us. When we are made aware of a certain address being used multiple times, we can always support law enforcement and other agencies like HMRC by providing data. The limitations are on our ability to do it proactively. One of the projects that we are developing at the moment is an ability for us to mine our data, when we have the appropriate powers, to identify suspicious activity. We will be running system checks all the time to try to throw up this information.

Some of the things are around reform with agents. I mentioned the need to verify. They will also need to create an account with us, which will allow us to check certain information and to cross-check our systems, hopefully to spot the kinds of things that you are talking about, where a virtual office has been used many times by the same people to create companies. They will also have to provide evidence that they are properly supervised, which, in effect, gives us a loopback to the supervisors, which we do not have at the moment.

Under the fifth money laundering directive, we now have discrepancies in PSC beneficial ownership information reported to us. The regulations and the Companies Act do not allow us to loop back to the supervisors where we see trends in discrepancy activity. We get the discrepancy, we can deal with it and we can seek to get the register rectified. If companies do not do that, we can go down the route of prosecution for PSC offences, but the big thing for me in the reform agenda is that ability for us as an organisation to loop back to the supervisors and to say, "We are seeing trends in activity that will be of interest to you. Here is the data."

Q146 **Alison Thewliss:** Is it not the case, though, that, in terms of limited partnerships, they are not going to be a single verified account in the same way? You cannot have limited partners registered in the same way as you can people.

Martin Swain: Yes, it is more complicated for limited partnerships, and we are working through it at the moment.

Q147 **Alison Thewliss:** That loophole needs to be closed; otherwise, people

are just going to continue to do that.

Martin Swain: I will pick up on a comment that Mark made earlier. We are thinking in Companies House about what systems we are putting in place and trying to close potential loopholes. In the same way as colleagues have said, we are dealing with very sophisticated individuals who are probably second-guessing our reform agenda, even before it becomes law. You are absolutely right that it is more complex for limited partnerships.

Q148 **Alison Thewliss:** If that is a loophole, they are just going to continue to use it, unless it is closed. This is not a new thing; this has been flagged for years.

Martin Swain: I totally accept that, and it is why we have to create a system that closes those loopholes.

Q149 **Alison Thewliss:** Coming to Simon and then to Mark, could you tell me a bit more about your assessment of the level of compliance in the sectors you regulate?

Simon York: We supervise nine sectors. They are very—

Alison Thewliss: You have broken up there. I cannot hear you. We will go to Mark.

Mark Steward: This is on money laundering systems and controls. It is one of our most significant programmes of work through both supervision and enforcement. We see strong compliance in most sectors that we regulate, but we also see problems and we see areas for improvement. In many cases, the problems turn into enforcement cases, of which there are a number at the moment. We have 44 current anti-money laundering investigations into firms' systems and controls.

The area that is most acute now is the crypto world. In January this year, we became the money laundering regulator for crypto-asset businesses in the UK. We do not regulate the businesses as businesses; we regulate them only from the money laundering perspective. All these businesses needed to register with us so that we knew who and where they were, and so that we could perform our job. At the moment, we are finding the registration process very challenging. We have registered five firms. We have a very large number of firms in the process of being authorised. The process of turning an industry that was unregulated into something that is regulated is very difficult.

Of course, we are taking this role very seriously and are very conscious of the association between cryptocurrencies and money laundering by organised crime groups. We do not want to end up registering the money laundering industry of the United Kingdom, so there is a very significant process on foot that we are engaged in, in looking at this industry and ensuring that the ones that are registered are as clean as we can make

them and we then regulate them properly from a money laundering perspective.

Q150 **Alison Thewliss:** In the March 2020 annual report, OPBAS found that 41% of professional body AML supervisors did not take any kind of enforcement action for non-compliance. It is a bit of a problem if those who are supposed to be taking that action are not following up. What further action is being taken to make sure that some of that happens?

Mark Steward: We would expect that those supervisors would be referring any instances to the law enforcement agency—depending on what was underlying it, potentially not taking action themselves but referring that to a law enforcement agency—because there may well be a predicate money laundering issue that also needs to be looked at. In any money laundering case where someone has facilitated money laundering because they do not have an effective system or control, there is a predicate offence that gives rise to the proceeds of crime that are being transacted through that system. It is really important that that also gets looked at. I can find out, but I would guess that, in many of the other instances, the matter has been referred to law enforcement.

Simon York: I would say that, generally, compliance is good across the nine sectors that we deal with. The majority of the businesses that we deal with are fully legitimate and really trying to meet all of their obligations. They take advantage of the educational work that we do and the guidance that we publish, and have very good controls and systems for protecting themselves against money laundering.

There are certain sectors that are higher risk than others. Money service businesses are the best example that I can give you. It is the highest-risk sector that we supervise, and we see an element within that sector that is very open to being used by criminals and sometimes complicit with criminals, and is certainly not fulfilling its obligations. There are some areas that are very non-compliant, which is where we will concentrate our resources and efforts.

Q151 **Alison Thewliss:** Graeme Biggar of the National Economic Crime Centre told us earlier this year that around 100 trust and company service providers create hundreds of thousands of new companies a year, and that the higher-risk formation agents tend to be those that are supervised by HMRC. They crop up repeatedly in the NECC's investigations. What action are you taking to reduce the risk of money laundering through those agents? Those ones are on you.

Simon York: Absolutely, and it cannot all be done by supervision. Part of the picture is, as Martin talked about, Companies House reform, and I would very strongly back what Martin said. If we can get that package of reform through, and through quickly, it will benefit all of us, giving Companies House extra powers as well as tackling limited partnerships and providing greater transparency of beneficial ownership of overseas entities. All of that will really help, and the supervision is part of that

picture. As I explained earlier, we have invested time, working very closely with Graeme Biggar and his team on this, in understanding which bits of that company service provider market are the riskiest, and then focusing our efforts on those. As I explained, virtual offices are one, and those providing multiple services are another, particularly when a service is connected, for example, with some legal or accountancy services—somebody who is planning the activity as opposed to someone who is just creating the company for somebody else. That is where we focus our efforts.

Q152 **Alison Thewliss:** Last year, only 31 suspicious activity reports were submitted by trust and company formation agents, which is very low, is it not?

Simon York: That is very low, and part of our strategy in that sector is to drive that up and educate the sector. As I explained earlier, we are going to do some webinars alongside the Financial Intelligence Unit in the NCA to try to improve that. That figure is a bit artificially low because some TCSPs are part of wider legal or accountancy firms and will be categorised within those sectors, so there probably are more than that, but I would agree with you that that is a low figure and we are keen to drive it up.

Q153 **Alison Thewliss:** What do you think the figure ought to be?

Simon York: It is impossible for us to say because we are not seeing the transactions that are taking place. We are not seeing the activity that takes place on a week-to-week basis. I would have thought it should be higher than that on the basis of what we do see with, as you say, the multiple creation of companies. It is quite difficult for some of these trust and company service providers and this is where we try to help and educate them.

For example, it is often the case that their immediate customer might be a trust and company service provider that is based overseas, and they will have done some due diligence on that customer, but it is the next step beyond that—the customer of that overseas body—that is the one they really need to understand more. It is not straightforward for them to do but we are really keen to build their understanding of how they can do that and how they can assess that risk.

Q154 **Alison Thewliss:** How effective are the newly resourced "policing the perimeter" teams with regard to identifying unsupervised company formation agents?

Simon York: Those teams are fairly new. They have made a good start. Identifying businesses that are unregistered and have not come forward is not easy, but we have good experience of doing that from a tax perspective. We have taken a significantly more proactive approach with this. Using web-based analytics is one of the big things we do to track down companies that perhaps are out there but have not registered with us.

Another big thing we have done is publish, in August 2020, for the first time, a fully open register of businesses. We encourage people to look at that if they have any suspicions and to refer businesses to us. We talk regularly to the trade bodies and to other businesses in this sector, and say, "If you have concerns about competitors who you think are not registered with us, refer them to us". That is a big step forward as well.

Another example here is a week of action we did with estate agents a couple of years ago. We targeted 50 businesses that we thought were trading but were not registered with us. We carried out unannounced visits in relation to those businesses. We then publicised the results from that, alongside a very big fine that we had levied on one of the country's biggest estate agents at that time, all with the aim of raising the issue and encourage the industry to get better.

We did a lot of work in trade magazines and that sort of thing that would get to that industry, and that has proved really successful. The number of those businesses that are now registered with us has increased significantly and almost doubled, from about 8,000 to about 15,000. That is not the only factor—there will be economic factors in there as well—but it has had a real impact. That is a model that we have used for other sectors and will continue to use.

There is a whole range of techniques that we use to identify unregistered businesses and to force or encourage them to be on the register.

Q155 **Alison Thewliss:** I want to ask Mark very quickly about those who are non-compliant within the OPBAS system. Under what circumstances would you use your powers to strip somebody of AML supervision?

Mark Steward: The effort so far has been to get the group of supervisors within OPBAS to understand the standards that they need to reach before we take such action. The reports that OPBAS has issued—and there have been two so far—have demonstrated the significant improvement that OPBAS has made to that group of supervisors. A third report will come out in autumn this year, which will demonstrate even further progress. We would need to see a supervisor having understood the standard and then to be failing to meet it, whether the failings are deliberate, negligent or incompetent—whatever the reason might be. We would need to see the standard not being met, now that they understand what the standard is.

It is reasonable for OPBAS to have spent its first two years and a bit in operation bringing the industry that it is looking at up to the standard that it needs to be. Now, having reached that point, we would expect that standard to maintained; otherwise, there ought to be action.

Q156 **Harriett Baldwin:** I wanted to turn to cryptocurrencies and talk to Mark about them. I just wanted to find out if you have prosecuted anyone yet for anything to do with cryptocurrencies.

Mark Steward: We became the money laundering regulator only in January this year.

Harriett Baldwin: So, since January, there have been no prosecutions.

Mark Steward: No.

Q157 **Harriett Baldwin:** Have you started to receive suspicious activity reports from crypto-asset firms?

Mark Steward: We do not receive suspicious activity reports. They flow into the FIU that is housed within the National Crime Agency.

Q158 **Harriett Baldwin:** Are you aware of whether it has received any?

Mark Steward: No, I am not aware.

Q159 **Harriett Baldwin:** Is that something that you could find out and share with the Committee?

Mark Steward: Possibly. The content of SARs is normally confidential, including the fact of SARs. Subject to the legal obligations that sit around SARs, I will endeavour to do that. There is another agency that has responsibility here for the FIU.

Q160 **Harriett Baldwin:** Is it not possible for anyone in this country to know if suspicious activity reports from crypto-asset firms have started to be received by the relevant agency?

Mark Steward: Generally, that is viewed as confidential information.

Q161 **Harriett Baldwin:** Can we not even know if they have happened at all?

Mark Steward: I will certainly find out whether I can tell you that. That will first involve finding out whether I can be told that as well. There might be someone more appropriate you could ask.

Q162 **Harriett Baldwin:** Is this one of the reasons why you have announced that you have extended the time limit within which firms can carry on business before approval to March 2022?

Mark Steward: No, that is not the reason. The reason is what I explained before: understanding whether these businesses are registerable to begin with or whether they should not be registered at all is a very significant process.

Q163 **Harriett Baldwin:** Should UK regulators be using innovation such as that used recently by the FBI—the secure app that was distributed to criminals and gave law enforcement agencies a back door to read their messages? Is that the sort of thing that we should be doing here?

Mark Steward: That is probably a question that you should be asking the NCA rather than the FCA, but, yes, it quite clearly is. In fact, the UK also shared in the fruits of that breakthrough.

Q164 **Harriett Baldwin:** I know that we did. I just wondered if it is something

that the UK regulators, either you or the NCA, should be doing proactively.

Mark Steward: Yes, and that does happen proactively.

Q165 **Harriett Baldwin:** Simon, can you talk to me about these very annoying texts, phone calls and email messages that we all receive and that try to get us to reveal our personal information, claiming to be from HMRC and often using HMRC branding? It is a problem that has been around for years. What is your assessment of the problem? Are we just going to have to put up with it or is there something you can do about it?

Simon York: First, I agree that they are very annoying. I have had a few myself, although I have not yet had the one that uses my own name in the scam, and I am looking forward to that moment. They have been around for quite some time. HMRC takes abuse of its brand very seriously. We do not want any individual to suffer because our brand has been abused, so we work with policing and others to see what we can do about this.

We have had quite a success. A few years ago, HMRC was the third most spoofed brand in this sort of thing internationally. Through a series of things that we have done, we have taken that out of the top 100, although it might not feel to those of you who have received some of these texts that that is what has happened.

In terms of the sorts of things we are doing, we get websites get taken down. We work with Ofcom to ensure that our official phone numbers cannot be spoofed. We work with law enforcement here in the UK and overseas, because some of these frauds originate overseas. We are doing a whole range of things to try to protect our customers. We also have a fraud reporting service where people can refer that. There is lots of activity going on and it is definitely something that we take seriously. It is not a fraud against the tax system but against citizens, and typically for the police to investigate.

Q166 **Harriett Baldwin:** Are you aware of whether they have been successful in catching any of these people?

Simon York: Yes, absolutely. There have been a number of criminal investigations where people have been caught and sent to jail, indeed. It is not always easy, especially if things happen overseas, but I am aware of some activity recently in another country, where, working with that country's law enforcement, a call centre was raided and a series of people arrested. That is the type of thing that is going on in the background.

Q167 **Harriett Baldwin:** Turning to the economic crime plan and the progress update that HMRC has made good progress on five of its six commitments, but that the planned increase in compliance interventions has not been met, can you update us on when HMRC plans to introduce a more proactive approach to supervision, particularly of trust and company service providers, and when the plan will be made public?

Simon York: We have definitely already introduced a much more proactive approach to supervision. Earlier in this session, I said that we were starting from a reasonably good foundation, as FATF had acknowledged, but we have been particularly proactive over the last couple of years.

I will just talk you through two or three things that we have done in the economic crime plan. We had agreement from Ministers to increase the fees that we charge businesses, which has allowed us to recruit an additional 100 staff, although not quite as quickly as we had hoped, because of the pandemic. We are now in a really good position to push on and significantly increase the number of interventions that we carry out. The plan is that that happens this year.

We have really tightened up our registration approach, which has resulted in 235 registration applications being refused during 2020-21. We have developed a whole new sanctions framework with the explicit intention of being much more robust, so that these sanctions are dissuasive, effective and proportionate.

Let me give you a couple of examples of what has happened as a result of that. In 2021, we have a higher overall value or penalties and a higher average value of penalties than ever before. In 2018-19, penalties totalled £1.2 million; in 2019-20, it was £9 million; and in 2020-21, the year just finished, it was £33 million, so you can see that that is really ramping up. We are suspending more businesses, and I mentioned the registration refusals as well. We are being increasingly proactive and robust in the way we carry out this activity.

As I said before, HMRC is slightly different to the other supervisors, because we are also a tax authority and an enforcement body, which we can use to our great advantage. If I look at what we are doing on the enforcement side, we have charged 100 people with money laundering offences over the last three years, 75 of whom have been convicted.

In terms of the proactive sort of thing that we are doing and that you might be interested in, I talked earlier about money service businesses being quite high risk, because people can literally walk into them with bags of cash and have them moved to wherever. The sort of thing that we might do is send in one of our supervision teams to have a look at their business and talk to them about their systems and processes.

At the same time, we might be carrying out covert surveillance on that business. When our investigators in the business are told, "We have 25 to 30 customers a day, which accounts for the throughput of value," our surveillance team has observed just three people who have been carrying bags that look like they are stuffed full of cash. We can then use that information and go a number of ways.

We could continue down the supervisory route and use some of the penalties or suspensions of that business, or deem someone to be not a

fit and proper person to run that business. We could go down the enforcement route, engage in a criminal investigation and end up putting someone in prison for money laundering. We could look at the tax side of things as well. We have a suite of powers and approaches, and I have teams with the skills and capabilities that can do all that.

That is what we have been putting our energy into over the last few years, and that is why the anti-money laundering supervision part of HMRC sits with me in our Fraud Investigation Service. My part of HMRC is 5,000 strong. We deal mainly with tax crime and tax criminals. We have put this bit in here because it is all part of dealing with fraud, and we can make use of all those powers and skills. There have been really significant changes in the way we are dealing with anti-money laundering supervision over the last few years.

Q168 **Harriett Baldwin:** It sounds like the lessons of Al Capone in the 1920s and 1930s have been learned.

You are one of the founding members of the National Economic Crime Centre. Can you tell us how that is going from your point of view and what could be done to improve its use to the regulators?

Simon York: The National Economic Crime Centre was set up just a few years ago and, as you say, we were one of the founding members. It is an organisation led by Graeme Biggar, who you had at your last session, and hosted in the NCA. It has been a really good development to formally bring together all the key players in the landscape of tackling economic crime. It has been useful in helping develop some policy options. The NECC has very usefully co-ordinated a number of significant operations. We have a number of staff embedded there. We work with them pretty much every day of the week, and I work closely with Graeme on a regular basis as well.

Q169 **Harriett Baldwin:** Specifically, what could be done to make it more useful?

Simon York: Part of that is time. It is a relatively new organisation, this is a very complex landscape, and it takes some time to get going. I know that, if Graeme were sat here, he would say that some more resource would help co-ordinate those organisations that I was talking about. I am not sure that there is anything that it needs to be more useful, other than the investment in time and resource.

Q170 **Harriett Baldwin:** Martin, some of the actions for Companies House in terms of the economic crime plan are not yet complete. Can you tell us why and when they will be?

Martin Swain: They have not been because of two actions: the reform of Companies House, and the register of overseas entities beneficial ownership Bill. Both are with the Department, and it is down to the Department and Ministers to decide, with colleagues, when we get the parliamentary slot. As I said in an earlier answer, we are transforming

our organisation, so it is ready to deliver on the reform agenda and to deliver the new register of overseas entities, but we can only so far without primary legislation.

Q171 **Harriett Baldwin:** When you say "the Department", are you talking about BEIS or Treasury?

Martin Swain: The two actions in the economic crime plan are for BEIS. They impact on Companies House. It is ultimately for Ministers to decide when we get parliamentary time.

Q172 **Harriett Baldwin:** Mark, what progress has the digital sandbox pilot, which was launched in October 2020, made in improving the private sector's ability to tackle fraud and scams? In your view, how effective is that programme?

Mark Steward: The programme will be enormously effective. We are still evaluating the results. As you say, it started in October last year. It is one of the initiatives under the economic crime plan that we are leading on, and we are in the process of evaluating the outcomes of that at the moment.

Q173 **Harriett Baldwin:** What should the public read into it? Can you highlight any good things that it has done?

Mark Steward: We are trying to work out exactly what the results are now, so it would be premature for me to talk about that. We are still working out what the results are.

Q174 **Harriett Baldwin:** Are you arguing for it to continue or are you waiting to see the evidence?

Mark Steward: We are testing the results. That is what I am saying. The sandbox will continue. It is an important part of what the FCA has been doing for a number of years now and the innovation that the FCA has been leading in financial services. We started work on this particular initiative that is part of the economic crime plan, which I think is the one you are referring to, in October last year. We are still evaluating what the outcome of that is.

Q175 **Harriett Baldwin:** Moving on to the Office for Professional Body Anti-Money Laundering Supervisors, can you summarise what meaningful action it has taken in the last 12 months?

Mark Steward: As I said before, there have been significant inroads by OPBAS into bringing the supervisors within the OPBAS framework up the right and consistent standard of money laundering supervision. In the report that it published in its first year, the assessment was that 10% of relevant supervisors were undertaking proactive supervision. In last year's report, that had jumped to 81%. It is a huge change in the way in which those supervisors are now operating, because of the work that OPBAS has conducted. We will see what the figures are in the third-year report, which is due to be published in the autumn.

These have been outcomes that have changed the way in which supervisors are operating. The purpose of OPBAS was not only to make the supervisors consistent in the way that they applied their approaches but also to raise their standards, so proactive supervision is clearly a very important part of that.

Q176 **Harriett Baldwin:** It is a bit shocking to learn that only 10% were doing it two years ago. Why would it not be 100% now?

Mark Steward: We will see what the report says this year, but an increase from 10% to 81% in 12 months is a significant outcome in itself.

Q177 **Dame Angela Eagle:** Listening to the evidence this afternoon, there are a couple of things that occurred to me. One is that this is a very complex and fragmented system that is trying to deal with increasingly sophisticated and costly frauds, to such an extent that we need a huge book of acronyms so that we can understand which institutions are trying to do it, let alone understand how effective it is. It is just very complicated. It also seems that the legislation you are working to is not really up to scratch. Mark Steward, is that a reasonable assessment?

Mark Steward: I will say one thing about the legislation that the FCA administers. It is commonly thought that we have a significant role to play in prosecuting fraud. In fact, the Financial Services and Markets Act does not contain any provision that gives us a function in relation to fraud, and the offences that we are authorised to prosecute do not include any offences under the Fraud Act. For a start, one of the things that create expectations around what we can do is, in fact, something that we are not authorised by the statute to do.

Dame Angela Eagle: I am sorry, but I think you are being a bit too defensive at the moment, if you do not mind me saying so.

Mark Steward: I can finish.

Q178 **Dame Angela Eagle:** My constituents who have been defrauded or are subject to increasing numbers of scams and risks across the system want to know that, if somebody scams them out of money, they can, if possible, get their money back and these people can, if possible, be convicted of fraud, put in jail and pay the price. They do not really want to know how the system works under the bonnet; they just want to know that the car drives. It seems to me that we have a very complex engine here that very few people can drive so it moves forwards.

Mark Steward: You asked me about legislation and I responded about legislation. I will now respond to that question. The challenge that we face, which I thought we discussed earlier, is that the increase particularly in online scams does not have an easily discoverable perpetrator, because the advertisements come from unknown people using false names and addresses. They are often not even in the country. By the time they have raised money from your constituents, the money is already out of the country as well.

We need to find a different way to tackle that phenomenon, because the prosecution powers that we have operate domestically, and they assume that there is evidence and that there are defendants within the jurisdiction who can be identified and found.

Q179 **Dame Angela Eagle:** Why is it that way? How can we get on top of this?

Mark Steward: We are using both ScamSmart and the warning list to tackle these scams in full flight, before they have found any victims. We are using the warning list to identify them in real time, so that both consumers, and banks and payment service firms that may be transacting the money, can be alerted to them in real time. If we cannot easily stop the increase in scams, we can do something to reduce the number of victims in the first place, including your constituents. We had to change our systems in order to do that, and it is the only way that we have at the moment of being effective in reducing the impact of scams and frauds on consumers.

Q180 **Dame Angela Eagle:** It is far more likely to be effective if it is the banks that block it, rather than expecting individuals to proactively look at a constantly changing list on the FCA website when they are being bombarded with adverts and scams that look very attractive and their guard is down.

I want to move on and ask you how effective Action Fraud is.

Mark Steward: We say to consumers, "Report to Action Fraud and report to us as well". We want to see the information ourselves directly. Action Fraud or something similar is an important way in which we can capture the size and extent of consumers who feel as though they have been defrauded, but it is not easily turned into action.

Q181 **Dame Angela Eagle:** It is inaction fraud really, is it not? Simon, what do you think of Action Fraud, because you also get sent reports?

Simon York: I am not sure that is really one for me.

Q182 **Dame Angela Eagle:** HMRC gets sent reports from Action Fraud, does it not?

Simon York: We do not have an awful lot to do with Action Fraud, no. It tends to deal with fraud against citizens. We are dealing with fraud against the tax system in the main. We have our own anti-fraud hotline and we get intelligence from all over the place. If there is something relevant, that will be circulated. We do not have a very big relationship with Action Fraud.

Q183 **Dame Angela Eagle:** Do you think it needs to be replaced? To me, it is almost just a telephone line. I might describe it as a gigantic black hole. Is that fair?

Simon York: I am not sure that is one I am best placed to answer, sorry.

Q184 **Dame Angela Eagle:** Can I ask you about SARs, not Covid SARS but the suspicious activity reports? There were 430,000 that came from banks last year and nearly 600,000 overall. With that many suspicious activity reports in the system, is it not impossible to think that it is useful, because of the sheer volume of it?

Simon York: It is certainly not impossible. The volume produces challenges, particularly for the Financial Intelligence Unit. Those SARs can be very valuable. We certainly use SARs as the starting point for many of our investigations, or as additional intelligence for existing investigations. We particularly use some of what are called defence against money laundering SARs, so the SARs banks send in before they might pay money away. We have used that particularly as a starting point for using account freezing orders. We have really scaled up the use of those over the last two or three years.

Q185 **Dame Angela Eagle:** It sounds to me like you actually use them because they are a way of looking up something, but you are already acting on other information.

Simon York: No, not necessarily. No, with the defence against money laundering SARs we might not have known about that at all. We will investigate that issue and then freeze those funds if we think they are related to criminality. As I said, they can be the start point for lots of investigations. It can be the first piece of intelligence. Yes, we also link it to other stuff. We essentially ingest all those SARs details and use them alongside all the data that HMRC has and uses to look at tax compliance generally. We certainly see SARs as a useful data source.

Q186 **Dame Angela Eagle:** Mark Steward, what progress have you seen in the SARs reform programme being undertaken by the UK Financial Intelligence Unit? Is it something that you think is going to produce dramatic improvements?

Mark Steward: It is a programme that we are engaged in. We would like to see more progress. The amount of data that flows into the FIU is large, but it is not beyond the ability to manage that size of data using the kinds of software applications and algorithms that now exist.

As Simon was indicating, in that context it is a valuable storehouse of intelligence that is useful when added to other information that we, the police and Simon get. On their own, individual items of intelligence that go into the SARs or the FIU database may not be enough to turn into action. It is only together with something else that it becomes really valuable. Sometimes, a very important missing link might be there.

Like Simon, we have also noticed an increase in defensive SARs being filed by banks. They are often rather more interesting. As Simon indicated as well, we have also used them as a launch pad to freeze money. We get a very limited space of time in which we can do that, under the process, but we have been doing that as well. It is a bit of a

mixed bag. More needs to be done in order to get more out of the valuable data that is in there. Otherwise, it just sits there.

Q187 **Dame Angela Eagle:** There is rather a lot of it.

Mark Steward: There is a lot of it. If I think about the other databases that we administer, we get a many-times multiple of that amount of data every day into our market data processor, where we analyse market transactions, looking for insider dealing and manipulation. It is a much bigger database, and yet we have the software to be able to analyse that in real time. The same can be done with the FIU.

Dame Angela Eagle: In that case, we can look forward to a huge increase in the effectiveness of the anti-fraud mechanisms that you are all fighting to put into effect very soon, if that intel database is as effective as you hope.

Q188 **Emma Hardy:** Thanks, everyone, for coming today to give evidence. My questions are around the resource challenges that you have with tackling economic crime. I will ask each of you in turn. The economic crime plan entails a lot of work across various Government agencies. Do you, as regulators, have the resources that you need to implement this?

Mark Steward: We certainly have the resources to tackle what we are doing under the economic crime plan. More generally, it is very clear to us that tackling economic crime across the spectrum requires all of us to work together. That is why the NECC is such an important part of the approach here. As Simon mentioned, if you ask Graeme what the NECC needs, it needs more resource. The FCA is also a founding member of the National Economic Crime Centre. We think the NEC needs more resourcing. It needs dedicated resourcing, so that that cross-partnership work that it is vital for all of us to be engaged in can happen more effectively.

Chris Hemsley: The APP fraud in particular remains a priority for the PSR. The resources that we have are not particularly the major issue there. I have talked about the issues around powers. I would agree with Mark that co-operation is key. The short answer is that the PSR's resources are not particularly the limiting factor on action here.

Q189 **Emma Hardy:** Can I ask you a follow-up on that one, Chris? What would your priority for additional resources be, if you were looking to do more than you are doing currently? Where would you want to put extra work and activity, if you had the resources to do so?

Chris Hemsley: I do not think the resources we have are particularly limiting what we can do. We need to take any opportunity for legislative action to address these issues around powers, which would allow us to move towards mandatory protection. We need to continue in our work, particularly around that prevention around confirmation of payee, making sure that we go from that 90% figure we have today towards addressing

the remaining 10% of the market that does not offer that important namechecking service that makes things harder for criminals.

Simon York: There have been a couple of recent developments on resources. I mentioned earlier that we have been able to increase the fees we charge to supervise businesses. That means we have been able to increase the size of our supervisory teams by 50%. That was very significant for us. In the latest budget, we also received investment to add about 400 extra staff to deal with illicit finances more generally, as it relates to tax crime and money laundering.

Overall, my unit is 5,000 strong. When I look at international comparisons and that sort of thing, we are reasonably well resourced. You can always do more with more. As others have said, tackling economic crime and tackling tax fraud is a very challenging job overall. I would support what Mark said about working together and the key role that the NEC can play in that.

Q190 **Emma Hardy:** You acknowledged that it is a huge challenge and there is always more you can do. To put it bluntly, are there any stones that you are leaving unturned because of the lack of capacity that you have? Are there particular things where you think, "I would like to do that specific action more", but unfortunately you cannot?

Simon York: HMRC is pretty experienced in dealing with fraud as it happens against the tax system. The key for us is flexibility in resource and being able to use the right type of approach as new frauds emerge. It is not always about throwing huge amounts of resource at one problem, leaving it on that problem and then saying, "We need more resource" for the next thing. You can move from one thing to another, to a degree, and use a range of approaches to try to drive down one particular fraud.

Mark talked earlier about preventing fraud happening in the first place. I would massively support that. That is absolutely our experience. Once money has gone, particularly gone to organised criminals, it is very difficult and expensive to get back. We try to build our experience in that, drive down one particular fraud and then move resources on to another. I think we are doing pretty well at that.

Q191 **Emma Hardy:** Do you have that flexibility in the way you have just described, the ability to quickly change as you see new frauds emerging and new areas of need? As an organisation, can you quickly divert resources and people in the way that you have just described?

Simon York: Yes, definitely. We have done this over an extended period. Probably the most recent example is with some of the Covid stuff. My teams had arrested people in relation to furlough fraud within three months of that scheme existing in the first place. That is a good example. We have done lots more since then and there is more to come on that.

That is a good example of how quickly we can use our experience to focus on something new.

Emma Hardy: Martin, what is your opinion on this?

Martin Swain: I mentioned earlier that we are in the second year of a five-year transformation programme at Companies House, which is a huge transformation of our digital systems, our skills and our ability to be that part of the economic crime system. We were allocated additional money in the spending round for this year, so we are carrying on implementing our transformation, I guess. The priority for us is to secure the funds we need to complete the five-year transformation, so once we have the legislative reform we are in a position to deliver.

Looking into that future, that will be a new function for Companies House. We will not be a regulator, but we will become far more regulatory in the way that we work, through things like querying information that is provided to us, rectifying the register, removing things, actively pursuing criminality. It is a different function. We will change as an organisation. It may well be that, once we have transformed, we will have a slightly different look to us. We will not be having lots of people doing processing work. We will have people doing much more intuitive work around keeping the integrity of the register.

The priority for us is to secure the money to do our transformation. In a few years' time we will then be asking, "Are we now resourced in a sustainable way in order to carry out that function in the future?" I know that, when the Treasury consulted on the economic crime levy, it indicated that some of the proceeds from that could come to Companies House to fund our enforcement work. We are keeping a really close eye on developments there.

Q192 **Emma Hardy:** I know that you have already had £20 million for some of the reform. Do you have an idea of how much more you need to fulfil your plans?

Martin Swain: It is about £75 million over the remaining three years.

Q193 **Emma Hardy:** What would happen if you were not able to get the funds you need to complete this work? Are you fully confident that that money is on its way?

Martin Swain: I am sure my colleagues with me today would agree that nobody can be confident in terms of securing money for budgets. We have strong support from the Department, in BEIS. We have strong support from Treasury, in terms of the need for reform. The simple answer is that we have a lot of legacy systems that are coming to the end of their working lives. If we are not able to migrate things off legacy systems, that will cause issues for us, in terms of service delivery.

Quite honestly, we will not be able to fulfil the role that Government want us to if we cannot change our systems and create the ability to operate

machine learning and artificial intelligence, as I think colleagues mentioned earlier. We have a massive database of 4.6 million companies, about 8 million directors and millions of people of significant control. Where Mark talks about the size of the database, it is huge.

We have done some work on it, in terms of abuse of the register. That was very manually intensive, on very small parts of the register, with lots of analysts spending lots of time. The value we would get back from the ability to do that in a machine learning way would be massive, compared to the investment.

Q194 **Emma Hardy:** That is really interesting, thank you. I was listening with interest to the evidence all of you have given. You have all given examples of how Covid has driven greater need. There has been more fraud online. We all have examples of constituents facing online fraud and the scams that are out there. It was really interesting. I think it was Mark who made the point that any one of us could be a victim of scammers. With all this happening at the moment and this increase, I am wondering what each of you is asking from the next spending review from Government to deal with these new challenges.

Mark Steward: We need to be continuing with what we have been talking about and making it more efficient. More money needs to be spent on law enforcement here as well. We have not really talked about the expectation gap that we all face as regulators, with the lack of priority that fraud really has for law enforcement. It is not their fault either because of the choices they need to be making as well.

It is enormously frustrating, particularly when we face a significant expectation gap between what people think we can do and what we can actually manage. That is why a focus on prevention, to reduce the number of victims, is super important. There are lots of small things that we can all be doing better, of course. There are lots of knives that we fail to catch that, in hindsight, we should have caught.

It all comes back to funding and the ability for all of us to work together. There is a huge amount of goodwill around this table, as there is among the members of the National Economic Crime Centre, but we need money to make things happen.

Q195 **Emma Hardy:** Do you have a particular figure in mind when you are saying that you need money to make it happen? Is there a particular figure that you are asking Government for?

Mark Steward: I am sure that we could come up with a figure, but I do not have one in my head right now. It would not be an enormous amount of money to enable the FIU to operate in a way like the FCA's market data processor, but it is an amount of money that is out of reach at the moment.

Q196 **Emma Hardy:** Is the lack of funding for that particular area having an impact on the service you are able to deliver?

Mark Steward: It means that data can sit there quite inert and cannot be manipulated in the way it can be through a sophisticated algorithm or some artificial intelligence. By itself, it will never provide you with the answer, but, in combination with other information that we all have, it might identify some of the more substantial drivers of this increase in particularly online fraud that we have seen in the last 12 months. That is a very significant objective that we all have, to try to do that.

Q197 **Emma Hardy:** I completely agree with your point about law enforcement and the need for resourcing in that area. I am running out of time, so I want to quickly ask a final question, if anyone is willing to step in and answer. In the last inquiry that the Committee did, it found that the public sector resources were inadequate for the problem. I wondered what your take on this was. Do you think private sector could do more to support and, if so, what?

Simon York: First, I would like to pay tribute to the people who work in the public sector. We have hugely skilled, committed and passionate people working, certainly, in my organisation and I see them across Government. They are probably people who could go and get paid more in the private sector, but do a fantastic job on behalf of the honest citizens and legitimate businesses of the UK.

Yes, working with the private sector is really important, and we do quite a lot of that through organisations like JMLIT, where we share intelligence and trends. That is good. We work with the private sector on technology. We have a number of technology partnerships in the law enforcement area and HMRC. The private sector has a lot to offer, but the public sector is full of very capable and hardworking people.

Q198 **Emma Hardy:** I completely agree, having worked in the public sector myself before being an MP. I agree 100%. You have pointed out an issue that I am sure we all recognise. People can earn more when they go and work in the private sector. In our previous Committee report, we found that the public sector struggled to retain expertise. Do you find that this is a problem because of those private sector jobs offering those higher wages, that you struggle to retain some of the expertise you have in your sector?

Simon York: We do in some very specialist areas, but not massively overall. There is always movement of people, as people move out of the private sector and people come from the private sector into the public sector. That is healthy. I have not noticed any dramatic acceleration of that. There are some niche, specialist areas where there is a bit of an arms race in terms of salaries. That can be quite tricky.

People work for HMRC for lots of reasons. Money is one of them. They want to be, and deserve to be, fairly rewarded. They also place great importance on the essential job they are doing to fund the UK's vital public services.

Chair: That brings us to the end of this session. Could I thank our four witnesses very much indeed for appearing before us today? We have certainly established that economic crime is rapidly growing. It is sophisticated. It is rapidly changing. It has taken advantage of the pandemic. It is entrepreneurial in its character in many cases. Its perpetrators are often highly elusive and that has led to an approach that is as much about taking down scams as it is taking out the scammers themselves, particularly as some of them are in other jurisdictions outside the United Kingdom.

We have also touched upon one or two areas where changes could perhaps be made to make the work that you and other agencies carry out more effective. We thank you very much indeed for sharing your insights with us this afternoon. Economic crime is a really appalling thing. The personal hardship that all the members of this Committee and I know that you, as regulators and enforcers, come across when we hear stories from our constituents is absolutely heart-breaking. It is really important that, collectively, we do as much as we can about it.

Mark, we had an interesting discussion when Rushanara was questioning you about the issue of Google and others, and the fact that the FCA is spending money warning people about some of the advertisers that are appearing on those sites. I think there was the question of £600,000 that was mentioned that you might be in discussions with them about, and whether they might return that to you. To the extent you are able to share that with us, the Committee would be quite interested in being kept up to date on that specific point and any other issues there might be around that, if you would be happy to do that.