Fraud Act 2006 and Digital Fraud committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 19 May 2022

9.20 am

Watch the meeting

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

Evidence Session No. 12 Heard in Public Questions 119 - 134

Examination of witnesses

Will Semple and Didi Denham.

Q119 **The Chair:** We are very pleased to be joined this morning by Didi Denham, who is the government affairs and public policy lead on advertising at Google, and Will Semple, who is a senior director at eBay. Welcome, and thank you both for joining. I will ask Lord Allan to open our proceedings.

Lord Allan of Hallam: Thank you. Just to set the scene I will ask each of you to describe, if you can, the types and volumes of frauds that you see on your platform, how those have been changing over time, what facilities there are for users to report fraud to you, and what happens when you get those reports in. I know you have very different kinds of platforms, so it would be interesting to compare and contrast between you.

If I could start with you, Will, can you describe the eBay types and volumes of fraud, what measures you have been taking, what impact you think those have had, what users can do if they think they have been defrauded through your platform, and how you respond to that?

Will Semple: Good morning, Lord Allan, and thank you, Chair, for the opportunity to provide evidence this morning to the committee. Let me start by just explaining a little bit of my own background. I am a senior director with eBay's global information security group. I lead eBay's

response to cybercrime globally. I have been working in this sphere for over 20 years and have held previous positions of seniority in the New York Stock Exchange for financial services, PwC with professional services and technology firms such as HP.

I would like to say that eBay takes fraud extremely seriously. In fact, every employee in eBay has objectives to help drive down the instances of fraud and increase trust on our platform. We do this, because ultimately eBay's marketplace is based on trust and we see fraud as something that undermines trust and impacts not just our business, but the livelihoods of our consumers and customers who use our platform.

In our experience we have seen fraud begin primarily off our platform, continue on our platform and then conclude off our platform. As a result, eBay has been working for a number of years, especially over the last three or four years, to increase its response to this type of fraud. My own team, for example, works very closely with outside agencies in the ecosystem, such as our NCA, the FBI and the Secret Service in the US, and police forces and agencies across Europe to tackle and pursue prosecutions of the bad actors that perpetrate fraud and cybercrime against our customers and on our platform.

The types of fraud that we see usually begin around what we call an account takeover or an ATO. An ATO is where a customer's identity has effectively been stolen. That theft of identity predominantly happens off-platform. For example, my own team pursues the identification and pursuit of stolen credentials—usernames, emails and passwords—off our platform very rigorously, and we have recovered and protected literally millions of our customers before they become victims of fraud via an ATO itself.

If an ATO is successful, often we see fraud happening in two main categories, either a buyer fraud or a seller fraud. We have put in place a number of mechanisms to help protect our customers from these things. For example, from a buyer fraud perspective, we have the eBay money back guarantee. As long as it is a validated listing on our platform, our customers can report to us in a number of different ways—I will explain what they are very shortly—that they have potentially been the victim of some form of buyer fraud, so teams like mine and our colleagues in risk and global assets protection and our legal teams will investigate the instance of fraud. If it is proven, we provide a money back guarantee to that customer.

We also seek to protect our sellers. Seller fraud is where our sellers are attacked by bad actors off our platform. They seek to take over their accounts in order to engage in activities such as collusion around buying and selling and money laundering. Sometimes we even see seller accounts being used as part of large networks to try to bypass sanctions. What eBay has done in the background is develop significant technologies to detect, mitigate and disrupt these types of activities very proactively on our platform. Seller fraud and buyer fraud are the two main categories.

There are many categories that go all the way down. We use acronyms that you may hear today, such as "significantly not as advertised" or not "significantly not as described", and that is where we can identify a particular item that may be on sale in our marketplace that does not match up to what the actual seller has said is for the sale when the buyer receives the item.

Lord Allan of Hallam: Thank you very much. In terms of volumes and particularly trends over time, as a committee we are interested in focusing on the things that are getting worse for people in the UK, which seems to be a lot in the context of digital fraud. Are there published numbers that tell us how many of these frauds are being reported through your platform, or numbers that you could share with the committee privately?

Will Semple: We would be very happy to share the numbers with the committee privately. In terms of sensitivity, we do not want to let the bad actors know just how good or bad we are on the platform. We work very hard to keep that type of activity around disruption and protection concealed from them. In the UK, we have a very small percentage of fraud, less than 1%. We can share the specifics of these numbers with the committee later on.

In terms of trends, certainly in recent years we have seen an increase in the volume of attacks against our customers, broadly driven by the transition to online digital retail and e-commerce. As a result of the pandemic, we have seen it spike or increase, certainly in recent times, but in my own area of expertise we have seen a major transition from high street retail-type crime to cybercrime.

Generally, from my own experience over the years, when the economy or society are facing some challenges, levels of cybercrime tend to increase. We are definitely seeing this in the volume of stolen credentials, stolen credit cards and so on, which are then tried to be used on our platform and taken off our platform again to conclude the fraud itself.

Lord Allan of Hallam: Thank you, that is very helpful. Those figures, which of course we will keep confidential on the basis on which they are being shared, would be very helpful for us to get that picture. If I can turn you now, Didi, from Google's point of view, what are the major kinds of fraud that you are seeing? Again, what kind of reporting mechanisms are there and what are the trends that you are seeing?

Didi Denham: Thank you, Lord Allan, Chair and committee, for having us today. As you mentioned, our platform and product differ slightly from eBay's, so if I may I will take a step back and explain some of that. We too have seen a rise in sophistication and a change in tactics by bad actors to exploit our platform, and we have had to adapt our response to that.

One area where we have done that particularly in the last couple of years is online advertising and how that works on Google, particularly on

Google Search. You might be familiar with the search results page. Someone types in a search, potentially for something like financial services, and they will be delivered a results page that has what we call organic results on the main part of the page, and at the top there may be a couple of advertising results, which are clearly marked as ads. They are important for our users to help find information about different products and services, and obviously for advertisers in the UK.

Those are used by SMEs and many small businesses across the country, but many of the large financial institutions will also take out Google Ads. In the last couple of years we have seen that this is an area that bad actors try to exploit. They might take out an ad on a particular term and try to get a user's details to use to potentially commit fraud off the platform. Again, we see this kind of weave on and off line, much in the same way as eBay mentioned. This does not necessarily take place all on our platform. What we have had to do in response to that is cut down on those types of advertising.

With financial services in the UK, we now require every advertiser who is targeting UK users on financial services to be authorised by the FCA. We implemented that change in September of last year and we have seen that have a very significant impact. It has been acknowledged by the chair of the FCA. I think in an article in the *Times* recently the TSB said that it felt that it had almost all but eliminated scams on Google Search, but I would stress that there is no room for complacency here. We know that these actors will try to circumvent systems, move to different platforms and move to different areas, so we are constantly evolving our approach. That latest change was the result of 18 months' work with the FCA in which we had introduced two new forms of verification. We updated our ad policies. That meant that advertisers were restricted in the rates of return they could advertise, or it stopped them from using terms like "guaranteed investments" or "guaranteed returns".

We have been receiving the FCA's warning list for the last two years. We receive that list from the FCA on a regular basis and take action to stop websites that are listed from using Google Ads. We found that the vast majority were not using Google Ads, but it allows us to take action and make sure that they cannot use them in the future. It is definitely an iterative approach that we are continuing to evolve.

Lord Allan of Hallam: I think other members of the committee will dig into the FCA approvals and the verification, but the final bit was about user complaints. If a user thinks that they have been defrauded because of an ad that they saw on Google Search, what is the process? What do you do? How can they get that sorted?

Didi Denham: There are a couple of different ways. The first is directly from the ad itself. If they see an ad and think that it does not look quite right, they can click the "About this ad" menu, which on Google Search looks like a small arrow, and they can choose directly from there "Report this ad". That will then go to our trust and safety teams, who will review the ad for compliance with a range of our policies and determine whether

it should be taken down. They can also, if it is after the fact, quite easily type in "Report a Google ad". They will be directed to a form and they can do it that way. Again, that will go to the trust and safety teams.

Lord Allan of Hallam: Thank you very much. Is there any data that you publish regularly or that you would be willing to share with the committee that gives us an insight into trends in relation to fraudulent activity through ads on Google Search?

Didi Denham: Yes. We publish an annual ads transparency report. We just published one a couple of weeks ago looking back on 2021, so I would be very happy to follow up and share that with the committee. That speaks to some of the trends we are seeing globally. We saw, for example, bad actors trying to take advantage of the Covid pandemic and that sort of thing. These actors will adapt their methods quite quickly, so that will give you some insight into the trends. That details that last year we took down 4 million accounts globally for things like misrepresentation, phishing or cloaking, so that type of fraud. It is important to remember that that number is global and that one bad actor can have several accounts, but I would be happy to follow up on that.

Lord Allan of Hallam: I imagine that will be very interesting. Thank you.

The Chair: Thank you very much. That is fascinating.

Q120 **Lord Vaux of Harrowden:** Thank you. One of the things we have been surprised by is how little we seem to know about the fraudsters, who they are and so on. That makes life much easier for the fraudsters to carry out the frauds, and it makes life much more difficult for those who are trying to prosecute and prevent it. What is your view on introducing more stringent know your customer-type checks, a bit like banks do, on advertisers and potentially other users using your platforms?

Secondly, what is your opinion of the measures outlined in the Government's digital identities trust framework?

Will Semple: Thank you. That is a great question. I would like to start with the myth of anonymity online in my area of specialty of cybercrime. There are several mechanisms and techniques that I and our partners in law enforcement in the ecosystem of online can take to identify bad actors and track them down. In fact, in eBay my own team does this regularly in collaboration with law enforcement not just across the UK but across Europe and US and further afield.

Your question about knowing your customer speaks very much to the heart of eBay's marketplace and our business. We seek not only to understand who our customer is, but to allow each of our customers to be trustworthy of each other. We spend a lot of time and a lot of effort putting processes in place around KYC. That stems not just from our obligation as a payments-regulated licensed entity, but because we fundamentally believe that the more that we know our customer, the

better the experience our customers can have on our platform as a third-party marketplace.

There are some things that we have done to increase our ability to know your customer. Over the last few years we have started to develop in-house our own processes, capabilities and manpower around identifying and working with know your customer as we onboard our customers as sellers on to our platform. In fact, we have lowered the sell value to kick off even more stringent reviews of who your customer is. Some of the things that we verify are simple things such as email address and telephone number. We can raise it up to verifying your address. As you become more successful on our platform as a seller, for example, we can then connect with the financial institutions and increase our verification of the financial transactions that are occurring from your account to your bank account. We do similar things with buyers to drive better KYC itself.

In terms of the proposed framework, eBay would be very pleased to participate and welcome such a framework. In fact, it aligns very closely with how we set our verification identity programmes inside eBay, and it would fit and connect very nicely. We would welcome it primarily because it provides stronger connections between industries and institutions in our ecosystem. The better we can make those connections, the more efficient connections we can make in identifying who are our customers are and preventing bad actors and sanction-breakers and so on from working, the better and more trustworthy our marketplace will be.

Lord Vaux of Harrowden: Interesting, thank you. Didi, your business model is rather different. We just heard from you a minute ago that effectively the FCA has changed things in terms of there is an area where you are now knowing your customer. Why do you not do that for all advertisers and all users? What is your view on that?

Didi Denham: Yes, that is a very good question. We have focused on financial services, but generally we have implemented know your customer-like checks on all our advertisers, or we are in the process of doing so. At the moment we are rolling out what we are calling advertiser identity verification for all advertisers globally. This process is well under way in the UK. That asks an advertiser to provide us with a government or state-issued ID and its business and corporation documents. That allows us to know more about it and to introduce a layer of friction that deters bad actors.

We have a second layer of verification that we can use, which is business operations verification. This is not for all advertisers, but we can use it where we suspect potential fraud or policy violations, where it might look like previous fraud that we have seen but does not quite violate our policies. In that second check we ask an advertiser to provide us with more information about its business operations. That might be third-party relationships or the product or service that it is selling. Those are applicable to all advertisers and, as I said, we are in the process of rolling out the ID verification globally to everyone.

Where there is a potential higher risk to users, we implement even more stringent checks. We have mentioned the FCA list for financial services in the UK. We also employ a similar method on areas like gambling, where we require registration with the Gambling Commission, or on pharmaceuticals or medical products. We are doing that. It is very helpful. It is one tool in our arsenal to defend against bad actors.

Our learning from that is just to make sure that those checks are proportionate to the risk of user harm, because we know that many SMEs use Google Ads, and often they are one or two-person operations relying on Google Ads to find new customers and grow their business, but implementing too stringent or time-intensive checks may deter them from advertising and give larger players an advantage. That is why we weigh it up, and where there is a higher risk we will employ even stricter verification methods.

Lord Vaux of Harrowden: Given that you are doing these checks, presumably I can read from that that you would not be averse to that coming on a more legislative basis—in other words, that you have to do those checks to protect the end user.

Didi Denham: As I said, we are rolling this out, so ultimately that is for government or Parliament to decide, but we have these checks at the moment, yes.

Lord Vaux of Harrowden: Any thoughts on the Government's digital identity trust framework?

Didi Denham: Yes. We welcome the principles of confidentiality and integrity. We hear from our users the importance of confidentiality and particularly examples like Ukraine, where confidentiality online is an integral part of security, so we welcome the framework. It mentions those principles. I think it is at an early stage, so we are definitely keen to continue working with government on this.

Q121 **Baroness Kingsmill:** I would just like to probe a little further with Didi about the financial services ads. Has this had an impact on your revenues, for example?

Didi Denham: Yes. I do not have a number to share, but we have had to calibrate on this issue. The FCA list and the FCA's authorisation, by its own admission, is not necessarily perfect. It is kind of jagged and its regulatory perimeter does not include all financial services actors in the UK. For instance, some businesses like SME lenders sit outside that regulatory framework, so this may have an impact on legitimate businesses that are able to advertise, but ultimately this is about ensuring that our users are safe on our platform. If they do not trust the ads that they see, they will not click on ads in the future, and that will have a longer-term and more detrimental impact for our business.

Baroness Kingsmill: So although you might profit in the short term from fraudsters, in the longer term it is not good for your business.

Didi Denham: Exactly, so we would rather take very strict measures to prevent that.

Baroness Kingsmill: If fraud is detected at all, what do you do to compensate your customers or the people who have been defrauded?

Didi Denham: Any user being defrauded on our platform is terrible and we try to invest as much as possible in making sure that no users are ever in that position. We work hard to make sure that we are investing in the processes, technology and people so that we are in a position where people are not getting defrauded on the platform.

Baroness Kingsmill: You do not have a compensation system.

Didi Denham: No, we do not, but we will invest in our systems.

Baroness Kingsmill: Just to go further, do you think that the system that you have in relation to financial services could be extended? You obviously co-operate quite well with the FCA. There are other regulators, not necessarily in financial services, but there are, for example, the energy regulators and things like that, and frauds take place there too. Do you have a similar sort of relationship with other regulators?

Didi Denham: Yes. We have a very constructive relationship with the FCA, and similarly with the Gambling Commission. As I mentioned, we do similar checks in gambling, pharmaceuticals and medical advertising. There is a possibility that we could talk to other regulators too. It is important that there is an authorised list that we can leverage. That is what has been so helpful about working with FCA: that it has this authorised list.

Baroness Kingsmill: So the regulator helps to protect you as well as customers.

Didi Denham: Yes. It helps to understand who is a legitimate advertiser and is allowed to advertise and who is not, so it is important to have that list.

Baroness Kingsmill: Of course the FCA regulates UK-based financial services. Google is a huge international firm, and a lot of fraudsters who are defrauding customers in the UK may be from firms outside the remit of the FCA. What do you do about them?

Didi Denham: That is a very good question. This requirement for FCA authorisation is for any advertiser wishing to target a UK user on financial services. It is based on where the user is. We require you to be FCA-authorised, so that is how we do it.

Baroness Kingsmill: That excludes quite a large number of international firms, one imagines.

Didi Denham: Yes, potentially, unless they are regulated with the FCA or have approval from an FCA-authorised firm.

Q122 **The Chair:** Thank you very much. I was going to turn to the Online Safety Bill to get the thoughts of both of you on the fraud measures that have been announced. The Bill is starting to be debated seriously next week. We have also had submissions so far to the committee that there should not be distinctions between the different platforms. Didi, I know that Google, as a search engine, is treated separately from other platforms. It would be good to get your thoughts on that.

Will, I do not know if you have a sense yet of how eBay will be categorised under the Bill, but perhaps we can start with you and your thoughts on the Bill and potential categorisation, Didi.

Didi Denham: Yes, thank you. As you know, we have been working closely with government and welcome the intent of the Online Safety Bill to keep users safe. We have not waited for these measures to be included, and we have adopted these kinds of voluntary measures based on the FCA list.

When it comes to the distinction between Google Search and YouTube, in advertising we are trying to understand the difference. There is an important reason for that for our organic content. The distinction in advertising is ultimately for government to decide, but we are implementing these measures already today. That applies to advertising across our products, so we will make sure that users are safe on both.

The Chair: Do you have a view on the reason? Why are search engines being treated slightly separately, particularly the category 1 platforms? Google is an enormously influential global brand, which reaches billions of people, and the potential for harm being caused, as we have talked about, by fraudulent adverts or other things that might be found on Google is enormous. Do you think it is right that there is a distinction between search engines and other platforms?

Didi Denham: It is ultimately for you to decide, but I think it is important. We have a responsibility, absolutely, to keep users safe from fraudulent advertising. That is something we are taking very seriously and are taking steps to comply with today. I think it is ultimately for you to decide, but we are not waiting for that.

The Chair: Will, as I say, do you have a sense of how eBay may be categorised and any thoughts on whether the measures in the Bill might assist you in your efforts?

Will Semple: Generally, Chair, we welcome the Bill. We believe that anything that helps protect our consumers and our customers from online harms is very welcome for eBay.

In terms of categorisation, I do not think we have enough understanding yet of where eBay would be placed in a category to comment specifically on that. However, we like a risk-based approach. We believe that focusing on the processes, being proportionate and allowing platforms to drive responses to online harms in a regulated piece of legislation is a good thing, ultimately.

The Chair: Both of you are big global brands. Do you have a view on the UK taking the lead on this legislation around the world? One of the comments we have had is that it is difficult if each jurisdiction decides to regulate the internet on its own. That would cause global brands like eBay and Google difficulty. Will, do you have a view on that?

Will Semple: First, I would just like recognise what we see from the UK. We see very strong leadership in our ecosystem from agencies such as the NCSC and GCHQ, which we work with fairly regularly. With the law enforcement partners in the Metropolitan Police and local police, even my local area—if you might have guessed, the PSNI—we pursue prosecutions and chase down people who cause harm to our customers. We do think that the UK is a strong leader globally in the fight against online crime and harms. Is it a challenge cross-border? Yes, it is, but I think we can continue to work hard to break those barriers down and show the right way to move forward.

The Chair: Didi, what about the UK having its own regulatory agenda separate from other countries you operate in?

Didi Denham: Yes, absolutely, we welcome the UK's leadership in this space. We know that many other countries are looking to the UK to understand how you are taking this regulation forward and how it will operate. There is complexity in the regulation, absolutely, but we are working through that and are absolutely committed to the UK and committed to complying with that regulation when it comes.

Q123 **Baroness Henig:** Can I turn to the Government online advertising programme consultation? What would both of you like to see in the Government's response to the consultation?

Will Semple: That is an interesting question, thank you. The advertising area is potentially not my area of expertise. My area is cybercrime. However, eBay would be more than happy to collaborate and contribute to the review of online advertising. Our advertising is primarily driven as a publisher and we run our own due diligence on direct relationships with advertisers that we provide. The vast majority of our advertising is provided by Google upstream from us in the form of text and words that get placed at the bottom of our listings, so we are really inside the value chain itself. However, as a small publisher, we are very keen to make sure that we can do the right types of due diligence. An increase in regulation is again welcome. It helps to increase the trust in our platform, which is central to what eBay stands for.

Baroness Henig: All right. So I need to direct this question perhaps more to Didi.

Didi Denham: Yes, thank you for the question. With the online advertising programme, the Government are seeking to bring more transparency and accountability to the online ads ecosystem, and we think that is a good thing—it can only be a good thing—and aligned with a lot of the work that we are doing. We welcome the consultation. I think

it is the importance of viewing this holistically and considering the full impact of any measures to online ads in the UK. We know that lots of SMEs, as I have mentioned, use online advertising. Many have come online for the first time since the start of the pandemic and have spoken about the importance of ads to find new customers, to export abroad and to grow their business. It is welcome that the consultation also acknowledges those positive benefits, and we would encourage Government to take a proportionate approach, bearing in mind those benefits.

They also reference some work that we are doing with the Advertising Standards Authority at the moment, which is starting in June. We are launching an intermediary and platform principles pilot, which are kind of voluntary measures to get tech platforms involved in trying to address some of the harms that they have mentioned in their consultation. We are looking forward to that too. Yes, we generally encourage the Government to consider proportionality. Providing clarity where they can is very important with any regulation, and being clear on where different players in the ads ecosystem sit and the control that they have, bearing that in mind when proposing measures.

Q124 **Viscount Colville of Culross:** Good morning. I want to ask about fake reviews. The Government, in their draft digital markets Bill, plan to make it illegal to pay for somebody to host or write a fake review. They hope this will stop users being cheated by bogus ratings. It has also been reinforced by the CMA announcing that it hopes to have new powers of enormous fines for global platforms that allow their customers to be similarly mistreated. Do you think these new laws will be enough to stop fake reviews and selling fraudulent goods? If not, do you think more needs to be done?

Will Semple: This is a very important question. I will start by explaining eBay's position on product reviews. Product reviews are not something that you find an awful lot of on eBay. We work on a feedback-based system, which is feedback on an actual seller, feedback on a transaction or a platform or feedback on some form of customer engagement between two of our customers.

Where we do see product reviews is around what we call a verified or a non-verified piece of feedback or a listing review. By "verify" we mean that we can match a transaction on our platform to a piece of feedback from a customer who has sold or purchased on our platform. For example, if you decide that you would like to purchase a second-hand phone from one of our refurb stores, we would match your feedback to that transaction and allow that feedback to be marked as verified from you on our platform. If, however, you decided to leave a piece of feedback about the actual phone itself but did not purchase it, we would mark that as non-verified. You are entitled to your view and opinion, and we encourage that on our platform. If we discover that there are fake reviews or fake feedback being posted, we have technology and attaching capabilities that seek this out and look to verify and remove it if it is not correct.

Viscount Colville of Culross: Do you think that model could be rolled out to other online platforms? There is an awareness that there are plenty of fake reviews out there, certainly on other platforms.

Will Semple: We think it is a great approach, because it connects the buyer and seller directly and allows the actual consumer or customer to leave their personal view on it, rather than a product-based review of whatever is being sold. We think it is great. If other platforms want to copy our approach, we cannot stop them, but we think it would be a good thing for consumers to have their voice.

Viscount Colville of Culross: Didi, when the Google search comes up you have a whole range of different platforms like Tripadvisor and people who do have reviews, and when you are trying to go through Tripadvisor it is quite hard to work out what is a fake review and what is not. Is there anything you can do to try to make sure that these fake reviews are stopped from appearing in your search engine?

Didi Denham: Yes. I cannot speak to Tripadvisor, but I can speak to the reviews that we may have on our platform, many of which are through Google Maps. As with anything, we want people to be able to trust reviews that they are seeing. Every review is moderated before it goes live, so it is sent for review on our moderation system. That uses a combination of machines and humans. We receive large quantities of content every day, so it is important that we have that kind of technology to review it at scale, but then also to have human moderators to make sure that we are capturing everything and capturing trends. Our latest stat, we believe that globally less than 1% of all content viewed on Google Maps is fraudulent, but obviously any amount is too much, so we continue to invest to try to ensure that those are not on our platform.

Lord Vaux of Harrowden: What about in those general search lists that come up? Is there anything more that you could do to try to discourage some of those websites from using fake reviews?

Didi Denham: Yes. That goes back to what I mentioned earlier. If there are advertisers who may have links to Trustpilot or other review sites on their websites, we have a policy that makes sure that people have to be able to click through to that to see that the reviews are true and real, and where someone says that they have a third-party relationship with one of these entities we can use that business operations verification that I mentioned to check and find out more information about that. We are conducting checks, particularly with our advertisers, to make sure that it is truthful.

Lord Vaux of Harrowden: What about the platforms that appear? I mentioned Tripadvisor. What is being stressed in the draft digital markets Bill, for example, is making it illegal to host these reviews. Will that be enough to knock out the fake reviews that disfigure some of these sites?

Didi Denham: I am afraid I cannot comment in detail on the digital markets Bill. It is not my area of specialty, but I can definitely follow up

with our views on that. We absolutely do not want fake reviews on the platform or appearing in searches, so we are aligned on that, but I can come back to you with the detail, if that is okay.

Q125 **Lord Young of Cookham:** My question follows on from Viscount Colville's and is about spoof websites and smishing, whereby you get a text message and are directed to a spoof website. Before we came online I typed into Google Search "Donate to Ukraine" and in 0.43 seconds there were 3,660 million hits. I do not expect Google to have validated all of those, but earlier this month the BBC did some research and found hundreds of spoof websites on "Donate to Ukraine" where some organisations were setting themselves up as Save the Children.

Didi, what steps do you take to make sure that these spoof websites do not appear on Google Search, and how quickly are you able to take them down?

Didi Denham: Thank you for that question. As we have mentioned, the search results page has two elements to it. The first is the advertising piece. I spoke previously about the checks that we can do there to verify the identity of advertisers and find more out about their business operations. Beyond verification, we have policies in place and we have large teams working to check that ads are compliant with those policies, so from that element there are significant checks in place. On Ukraine in particular, we can implement sensitive events policies, which prevents people from being able to advertise on certain terms as well, because we know they may try to take advantage of that.

On what we refer to as an organic search, the second half of the page, again we are completely aligned with trying to ensure that those are the best results possible. That is why people come to Google. That works in a slightly different way. We do not host that content; that is just what is on the internet. But we do have Webmaster Guidelines on Google Search to ensure that people get the best possible results. I can follow up on the details of that particular investigation.

Lord Young of Cookham: How quickly are you able to take sites off your search engines when somebody tells you that they are fake?

Didi Denham: I do not have a number to share. I think it would depend on whether it is advertising or organic and if we are alerted by law enforcement that it is illegal, but organic works in a slightly different way.

Lord Young of Cookham: What about the organisations that use special search engine optimisation tools to appear right at the top of Google Search? Are any steps taken to ensure that that is not being abused to get these fake ones right at the top of the search?

Didi Denham: Yes, absolutely. We update our algorithm many times a year to ensure that that is not happening. Many legitimate businesses use search engine optimisation, but it is to ensure that scamming results are not appearing. Last year we made a couple of changes that meant there was a 40% reduction in scamming results between 2020 to 2021, so we

make every effort to ensure that the search results people get when they come to Google are the best.

Lord Young of Cookham: A quick question to eBay. I understand that quite a lot of organisations set up spoof eBay sites. What is your response? What steps are you taking to make sure that those are closed down quickly?

Will Semple: Thank you for the question. This is very close to what my team specifically in cybercrime in eBay does. If I can go back to the start of the question on smishing, you quite rightly made the connection between receiving a text message with a link in it and, when a customer clicks on the link, it often taking them to a third-party website or to a search page, where the listing of the fake and scam page sits. My team has worked very hard over the last few years to develop very innovative and unique technology specific to eBay that allows us to detect very quickly the existence of these pages and then work in our partners and ecosystems, including Google, to issue takedowns as fast as possible.

We also work with telcos across the US, the UK and Europe, where we identify the senders of these phishing/smishing texts to begin with and we take down the numbers or the virtual numbers that can be operated from anywhere in the world. We take this positioning of scam/fake eBay pages extremely seriously and proactively, and continuously develop new technologies and new techniques to detect, identify, disrupt and take down the pages as fast as we can find them.

Lord Young of Cookham: Is there good co-operation from the telecommunication companies?

Will Semple: Broadly, I would like to say that our ecosystem, which includes Google, is very co-operative. I partner with my peers in Google regularly and we partner at executive level as well. We identify and recognise the problems and the harms this causes our customers and our businesses.

In terms of the telcos, yes, we do partner in telcos in the ecosystems. Thankfully the majority of our telco partners and ecosystem partners react as fast as they can. There are some instances where some telcos may not act as fast as we would like them to, but ultimately we can bring to bear our relationships with local law enforcement and agencies in those territories to encourage them to remove the offending numbers.

Q126 **The Chair:** I will just follow up on that last point about the telcos, because it has come up quite a bit in our evidence. Will, you are covered by parliamentary privilege here, so if you want to tell us about companies that are less than co-operative, or if you want to tell us privately, that would be very helpful, because I think it would be fair to say that from a lot of evidence we have the telcos are not responding swiftly enough.

I appreciate that in giving evidence it is good to be polite about one's partners, but there might be evidence or information you have that can guide us to those who are not acting swiftly enough and not shutting

down the numbers when they know that there is a problem. Can I tempt you to say anything further on this?

Will Semple: I think this is the difference between now and five years ago. The ecosystem and our partnerships and relationships in the area of cybercrime, fraud, digital identity and so on that we work in, and the recognition in how we collaborate, share information and take proactive action has improved significantly. For example, eBay works very regularly with Google to take down what we call SEO phishing internally. We have people dedicated to this form of attack against our customers.

I can share some details perhaps privately, but I would just like to reinforce the fact that predominantly the ecosystem is proactive and we collaborate and work very well together.

The Chair: You also mentioned the ecosystem and working with law enforcement. Again, it will not surprise anyone to know that we have had evidence that this is just not Action Fraud's or local police forces' area of expertise. Again, do you spot that some law enforcement agencies are swifter to respond to your requests for help or the information that you pass on and follow it up, whereas some do not?

Will Semple: What eBay try to do is make sure that our consumers and our customers in the territories that we operate in can communicate to us and to the best local agency in their area. For example, we would often guide UK consumers to reach out to the NCA. If it is the US, it is the FBI cyber division. Some police services across the territories are more sophisticated than others. If we look at the volume of fraud and how much traditional fraud has increased versus digital fraud, we will see that cybercrime is a big driver in connecting to that digital fraud. Perhaps some of the resources from fraud overall need to be reprioritised in that direction to enable our police services and agencies to be upskilled more broadly across the scope of all activities.

The Chair: Thank you, that is very helpful.

Q127 **Lord Vaux of Harrowden:** We have heard from both of you how you identify and take spoofing websites off your platforms or whatever, but part of the problem is presumably how easy it is for people to set up a fake website, obtain a domain name and an address for it. Do you have any thoughts about how that might be made more difficult for fraudsters?

Will Semple: That is a very insightful question, and I appreciate it. This is getting to the source of phishing sites, scam websites and so on. They have to register a domain. Often they have to register what we call an SSL certificate, which encrypts the traffic between the web server and the customer's browser. This does not make it more difficult for us; it just creates a very interesting signal for us to keep track of and identify. In eBay we are developing technologies to do that very thing. We are developing how we get to the source of the establishment of these domain registrations and these SSL certificate registrations; how we can prevent these sites from coming up in the first place or as close to that as

possible. That is quite a sophisticated set of technologies that we are developing for this problem.

To your question, my view is that it is too easy to register, and some simple know your customer-type techniques would probably introduce a major speedbump into the entire process. They would not stop it, but they would definitely make it harder for bad actors to carry out these activities.

Lord Vaux of Harrowden: Didi, do you have anything to add to that?

Didi Denham: Yes, I would agree with what has been said. As Will mentioned, it is an insightful question. There is no one silver bullet to this issue, so it would be helpful if there were potentially stricter checks, but all parts of the ecosystem need to play their part in this.

Q128 **Lord Sandhurst:** Without your respective agencies and people like you, bad actors would not get access to the punters. It is also plain that you have both said that you do not want bad actors and that it is not in your business interests for there to be fraudsters out there, that it is bad for your image.

It is clear to me that the only people with the capacity to take steps to reduce the incidents of bad actors are you. Would it not be reasonable to put an obligation on you and others like you to take steps to prevent fraud? That obligation, which would be enforced by a regulator, whether it is the FCA, the Competition and Markets Authority or whoever, would have power to levy fines. You would be able to discharge that, but the burden would be on you to show that you had taken reasonable steps. Why is that not a sensible way forward: providing the commercial incentive for you to do it? It might put costs up slightly, but that is spread across all these transactions.

Will Semple: This is a very important question. The complexity of the online environment drives this into being a shared responsibility. Absolutely, eBay has a component of that responsibility. As I mentioned, a lot of cybercrime fraud begins off-platform, happens on our platforms and then gets concluded off our platforms.

From eBay's perspective, we would like to see it being risk-based and proportionate. We believe fundamentally that trust in our marketplace is at the heart of our business. We believe that we have a genuine moral, not just legal, business imperative to try to make our marketplace as safe as possible. As a result, we already take a loss from every time one of customers is defrauded on our platform. I mentioned the eBay money back guarantee.

This drives an awful lot of our thinking internally in eBay: how do we make our platform safer; how do we make it more robust; what are the processes that we can bring into play in order to make that less attractive to bad actors in the broader global ecosystem of digital and e-commerce? As long as we can make it proportionate and focused on robust measures and processes that we engage in, generally eBay has stated that we are

comfortable to move forward with it, but it is not in an individual platform's realm to solve fraud. It is an absolute shared responsibility.

The Chair: Didi, how about you?

Didi Denham: As you mentioned, we absolutely have a responsibility to our users to keep them safe when they are on our platforms, but there should be an incentive to take measures voluntarily to tackle fraud. I have spoken about some of the measures we have taken today, and we are pleased to see that others in the industry have said they will follow suit as well. It is encouraging that there is a voluntary process in this space. I note that the Online Safety Bill, which we have discussed, has introduced measures on fraud and fraudulent advertising, which we will of course comply with. That will introduce new requirements on us. Just to echo Will's comments about proportionality, it is considering the impact on legitimate businesses operating in this space.

Lord Sandhurst: You are the people who can do it and this is your business. To prevent bad actors intervening by advertisement, when someone is defrauded or there is a pattern of fraud you should take such reasonable steps, and if you do not you will have to pay the regulator a hefty fine. As I understand it, some years ago in America, Google had to pay a large fine because of the marketing of unregistered pharmaceutical products. Why would that not be a reasonable model for advertisers generally?

Didi Denham: As I have mentioned, we implement verification checks on all advertisers and policy checks before and while ads are live. We do that today, and I think that would be categorised as reasonable measures. As I mentioned, the Online Safety Bill will introduce further measures on that as well.

Q129 **Baroness Bowles of Berkhamsted:** Of course, it is not just your organisations that are involved, as Will has said. If there were some "failure to prevent" type of legislation, that might encourage people in the ecosystem to take greater interest. Would it not also provide some baseline for whether compensation is due, as has perhaps been touched upon? The consumers who have fallen for something may feel a bit less bad about it if at least they know that there are rules in place and that checks have happened, and that if there are not strong enough and diligent enough checks they would have a right to complain somewhere and a yardstick against which that could be measured. I am sure that would have to involve the kinds of things that you have talked about, proportionality and so forth. Would it be such a bad thing to have that enacted?

Didi Denham: Yes, on the progress you mentioned and encouraging others, we are pleased to see that others, as part of the Online Fraud Steering Group, have announced that they will take similar action to what we are doing at the moment. As mentioned, we are entirely incentivised to make sure that users can trust and have a good and safe experience on Google. That is where we invest our time and energy: in making sure

that is the case. We would comply with any future law as well as it stands.

Will Semple: I think the broader ecosystem from eBay's perspective includes our partners in payment services providers, financial services institutions, software providers and even name registrars for domains and so on. Everyone has a role to play and we cannot solve this individually. We must be able to solve it in the entire ecosystem and across borders globally as well. I also recognise that there are a number of regulations and legislation already in play that can be leveraged by our partners in regulators and law enforcement to help encourage good behaviour. If we want to improve upon that, I would hope that we could make it proportionate and risk-based and focus on the actual attacks against consumers, our customers, in our territories.

Baroness Bowles of Berkhamsted: If there were legislation, do you think there is a risk in trying to get guidance about what is reasonable? That is always a consequence of introducing legislation. Everybody says they want a principle, but the next thing they want is a set of rules. If there were some kind of set of rules made, do you think that would itself introduce risk, in that the people who were fraudsters would look at the rules and devise around them?

Will Semple: My own view, from experience, is that that is exactly what they will do. My expertise is on the front line dealing face to face with these bad actors on a daily basis, and they absolutely look to game the system. When we focus our response on process and on collaborative inclusion across the entire ecosystem, and we drive the disruption and the bar for cost to the cybercriminal fraudster up collectively, it decreases the exposure to our consumers from attack. When we set out too specific sets of rules, it gives them one idea of what the game is and what the playing field looks like, and we want to avoid that.

Baroness Bowles of Berkhamsted: Could you sit with a "failure to prevent" type of offence that was kept at a level that merely defined that you had to have had reasonable checks, allowing for proportionality, but without a set of rules, so that basically if you were tested by the regulator, it would be to see that you had kept sufficiently on your toes?

Will Semple: If I can draw a parallel with how eBay, payment providers and other audited infrastructures and platforms currently operate, we have a set of checks/audits that are carried out. From my own experience, there is a set of technical and security standards that have to be met, and we get audited on those every year to prove that we can do the robust responses and protections needed. Specifically, it really depends on the detail of what that would look like.

Didi Denham: I think it would be good to understand fully the details of that, but, as mentioned, there is a lot of work going on voluntarily in this space at the moment.

Q130 **Lord Browne of Ladyton:** Thank you both for your evidence thus far. I

think all my colleagues will have found it interesting and helpful in many respects. This question is about data-sharing. If I may, I will start with you, Will, because we are left in no doubt that you and your business have a very well-developed sense that your business stretches across the tech sector and that you are part of an ecosystem beyond the tech sector and into law enforcement. You have told us on more than one occasion, and I am convinced by it, that you accept a share of the collective but also individual responsibility for trying to interdict or investigate and stop fraud in that whole ecosystem.

I think you will agree with me, because you made reference to this on a couple of occasions, that data-sharing on fraud risk and fraud identifiers in that ecosystem is fundamental to your ambition to rid the ecosystem of this fraud. What regulatory, legislative or cultural barriers do you face when sharing data or asking that data be shared with you?

Will Semple: This information sharing is very close to my personal desire for the industry to get better in what we do. I will explain a bit about what eBay does with examples. A number of years ago, eBay developed its own internal law enforcement portal. We provide access for law enforcement agencies around the world, which gives them a direct channel to engage with eBay on specific investigations, and as a result we have the ability to receive requests for information, and to proactively share information, signals and indicators of fraud or cybercrime with these law enforcement agencies around the world.

In fact, when we work with our partners in the US and the FBI local law enforcement agencies at a state level, North America includes Canada. The Secret Service allows us to move across borders where the US has interests in the UK. We do it with the NCA and local police forces, and in Europe we do it with Europol, Interpol and, again, local state and territorial law enforcement agencies. This allows us to proactively share information. We bring packages of data to agencies where we want them to pursue a prosecution for fraudsters and cybercrime criminals we have identified ourselves. We are not in a position to execute the prosecution ourselves. That is why we must partner. It sends a very clear message that eBay does not sit back and take what happens in the broader digital online space lightly.

In terms of barriers, again, this is a continuously evolving story. Ten years ago, it would have been very difficult to share any information between two industry partners or competitors. When the likes of Anonymous attacked, I was with the New York Stock Exchange and leading the response to that. The financial services industry stood up and said, "We need to share this information, because this is critical to our collective defence and it is important that we do so".

If I fast-forward to where we are today, yes, there are still barriers, there are still challenges, in moving data across borders, which speaks more about the privacy legislation and how we can work in that to protect our consumers and customers' privacy while pursuing the sharing of information for prosecution, but generally the culture that I can speak to

is that people understand that we need to share information. How we share information is now the critical element. The desire to do it is definitely there, from my own personal experiences.

Q131 **Lord Browne of Ladyton:** If I may turn to you, Didi, it is perfectly clear, at least from what Will told us, that in the sector there is sharing of data between his business and your business—at least he made general statements about that—so there is some data-sharing going on. What is your business's experience of sharing data about fraud risk and identifiers in the tech sector, across the tech sector and with law enforcement?

Didi Denham: Just to take a step back for a moment on when we think about data-sharing or intelligence-sharing on fraud, there are unique challenges when it comes to doing this with fraud, in that it is deliberately deceptive by its nature compared to other areas such as violent extremism, where it is more straightforward to look at a piece of content and decide whether it is violative or not. Fraud kind of weaves on and offline and, as I said, is deliberately deceptive, so there are some particular challenges to this. That is not to say that there is not a space for it where there are appropriate safeguards for user privacy and potentially commercially sensitive information for advertisers.

There is lots of work going on in this space already. As I mentioned, we have the FCA's warning list, which we receive on a regular basis, which allows us to take action on our platforms. We have a similar system in place with the Advertising Standards Authority, where it can tell us about scam ads and it alerts platforms to that. When it comes to telcos and mobile networks where a user tells us about a scam text message that they have received, we are then able to share that back with telcos. There is work going on in this space at the moment, and it is important to consider how we can use the forums we have today, like the Online Fraud Steering Group, which has brought together the tech platforms and the banks to understand what more can be done.

Lord Browne of Ladyton: Can I take advantage of this opportunity with you just to clarify something? I am not entirely sure that I understood your evidence earlier when you were talking about the distinction between organic data and data that had been paid for as ads and how you treated them. Take, for example, the FCA's approval of people who are trading crypto assets. A very limited number, less than 10% of the people who are doing business in this area in the United Kingdom, are approved by the FCA to do it. You have to be approved by the FCA to do it under money-laundering regulations and terrorist financing regulations. I presume that you would not accept advertisements from people who are not on that very limited list, which is 10%. I just take it for granted that you would not, but if an organic search brought up one of these businesses, a product, you would leave it in the organic search, because that is already on the internet. Is that right?

Didi Denham: Yes, basically if it is there, because the organic search works in a slightly different way in that it is not administered by Google; it is just kind of an index of what is online.

Lord Browne of Ladyton: How would I know, if I searched for a crypto asset business, that these people, who are in no sense rated in their businesses, are not people you would accept ads from because they are not compliant with the law? I would not know that.

Didi Denham: I think that is where there is room for user awareness and scam awareness, or financial awareness campaigns for users. We have contributed $5 million—about £3.5 million—of ad credits to the likes of the FCA and the ASA to raise awareness among consumers about the risk. I know that the FCA is doing a lot of work in that space.

Q132 **Lord Browne of Ladyton:** I have another question about data. What more data would you find useful that you could get from other tech businesses, from law enforcement or from the financial services industry if there was better collaboration in and across sectors? Do you have any desire to get any more information to make your interdiction of fraud better?

Will Semple: I think it is contextual. There are some basics that we already are aware of that we can discuss to do with signals. I would prefer not to mention what those are in an open forum, but I think it becomes contextual, depending on the specific type of cybercrime or fraud. That then passes this into which part of the ecosystem is in play. I would not say there is one default set of enhanced data that we could get, broadly. I think it is more the cultural desire to work together in order to identify the right type of data at the right point in time to our lawyers to pursue the next step of the investigation and research.

Didi Denham: I would agree with that. Unfortunately, there is no one silver bullet to this. As Will mentioned, it does not depend on where a platform sits in the user journey of the scam, but I am encouraged by the fact that there is work going on in this space. There are forums, which have been set up in the last several months, that will bring together all the relevant industries, so I am encouraged by that progress and hope to see more action in the future.

Q133 **The Chair:** Thank you very much indeed. We are almost at the end of our time. I have one supplementary for Will and then I will ask for one policy recommendation, if you have one. Will, we talked earlier—I think this is probably more relevant to you than to Google—about working between partners. I wondered if you had any thoughts on working with different financial services, banks or payment providers. You talked about the fraud in eBay often starting offline, coming on to the platform and ending up off the platform. I presume that last stage relates to payment or somebody realising they have been defrauded and whether they can get their money back. Do you work with the banks or other payment providers? Again, how responsive do you find they are?

Will Semple: Indeed we do. In fact, I will explain it in two different ways. The first way specifically in the UK. Colleagues in my team are a member of a UK programme called CISP, which is an information-sharing programme run by the Government. We specifically contribute and are

members of the retail and payments sub-groups, which allows us to work very closely with members of the payment providers, financial services, banks and so on to allow us to share information very quickly and specifically.

On the question of whether there are good banks and good payment processors, and ones that are not, broadly I would say no. The payments are regulated with payments licensing. We believe in more than just regulation, and that it is the right thing to do. Sometimes financial products such as virtual cards cause challenges that delay investigations. This is where the likes of privacy legislation collide with our ability to tackle and combat cybercrime and fraud. We can only see a little portion of a virtual card. We call it "running on rails", the rails of the bank that owns it, so it is a bigger challenge for us to move that downstream and get to some good data that allows us to pursue the investigation to the next stage. That is probably the most pertinent challenge we see at the moment, but certainly the UK banks are quite responsive and very open to working with us.

The Chair: Didi, how about Google's relationship with banks or payment providers? Obviously it is a very different business model from eBay's.

Didi Denham: Yes, it is slightly different, but we do have relationships with the banks and, as I mentioned, through the Online Fraud Steering Group we are a member of Stop Scams UK, so we speak regularly with the banks about what more we can do to collaborate in this space.

Q134 **The Chair:** Finally, we have touched on a number of things where you have both said that there is room for improvement or that things might change. Will, in the job that you do, is there one policy recommendation to government that would make life easier and help to keep consumers safer?

Will Semple: Yes, and I have mentioned it a few times before. I think the biggest thing is how we fund the resources for fraud broadly. Certainly we see a lot of activity on fraud, but when we look at the growth of digital fraud and cybercrime in the space itself, we see perhaps that it is, on balance, where the majority of actual victims reside versus the volume of capability and resources available broadly in fraud itself. If there was one recommendation that certainly eBay would like to see, it is perhaps a rebalancing of where the majority of the victims are, which is in digital fraud versus traditional fraud. That would be helpful.

The Chair: In terms of the resources, you are talking about law enforcement and the agencies?

Will Semple: Yes, exactly. We work with these guys every day and we see the dedication and the effort that is going into it, and we cannot deny it. We just wonder how much more effective everybody could be if there was a rebalancing of where the victims reside, which is more in digital than traditional, as I said, and how much more we could do.

The Chair: Didi, one recommendation.

Didi Denham: It is a similar answer. As we have touched on today and I know your committee has heard in previous evidence sessions—the Treasury committee has conducted a similar inquiry, I think—more resources can only be a good thing to help us work collaboratively. We all have a role to play in this, but more resourcing can only ever be a good thing.

The Chair: Thank you very much, both of you, for giving evidence and your time so generously this morning. We are very grateful for all the points that you have raised and it has been thought-provoking. There were a few points where we talked about perhaps further evidence coming in privately or being followed up, so the team will follow up with both of you about that. Thank you very much.