

Treasury Committee

Oral evidence: [Economic crime](#), HC 145

Wednesday 22 September 2021

Ordered by the House of Commons to be published on 22 September 2021.

[Watch the meeting](#)

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

Digital, Culture, Media and Sport Committee Member also present: Julian Knight.

Questions 267 - 426

Witnesses

I: Amanda Storey, Director of Trust and Safety, Google; Will Semple, Director, Global Information Security Team, eBay; Allison Lucas, Content Policy Director, Facebook; Gaon Hart, Head of Public Policy, Customer Trust, UK & Ireland, Amazon.



Examination of Witnesses

Witnesses: Amanda Storey, Will Semple, Allison Lucas and Gaon Hart.

Q267 **Chair:** Good afternoon and welcome to the Treasury Committee's witness session on economic crime. We are focusing today on online platforms. I am very pleased to welcome to our Committee Julian Knight, the Chair of the DCMS Committee, who has been invited to join us under Standing Order No. 137A, which gives us the power to do that. Welcome, Julian. Thank you for joining us today.

We are also joined by a panel of four witnesses, two of whom are present in person, with two joining us remotely. Could I just ask all four witnesses to briefly introduce themselves to the Committee?

Amanda Storey: Hi, I am Amanda Storey from Google, and I am here representing the Trust and Safety Team, which operates globally to protect users on our platforms.

Gaon Hart: My name is Gaon Hart. I have spent 30 years as a specialist fraud and corruption expert, including working as a prosecution team leader for the Crown Prosecution Service and as a senior Crown advocate for the special crime and counter-terrorism division. I am here today representing Amazon as the head of UK public policy, developing relationships in order to address fraud and scams.

Allison Lucas: Hi, my name is Allison Lucas. I am a content policy director at Facebook, based in New York City. My expertise here is in content policy, where I oversee unpaid policy development work as well as commercial advertising policy development work.

Will Semple: Good afternoon. I am Will Semple, a director with eBay's global information security group. I have 20 years of working on the front line across both public and private sector financial services, dealing with cybercrime and fraud.

Q268 **Chair:** Thank you and welcome to all of you. There may be some Divisions of the House during this session; in fact, there might be one fairly soon. As and when those arise, I will just suspend the Committee for about 15 minutes, if it is a single Division; perhaps a bit more if it is more than one Division. If I can ask all witnesses just to remain in place, we will come back to you in that event. Thank you very much.

For my first question, I would like to start with Amanda. There has been a huge rise in online crime. I wonder if you could share with the Committee your understanding of what you think it is all about, what is going on, particularly in relation to your own platform when it comes to fraud and online crime, and what your company is doing about it.

Amanda Storey: Scams and fraud are organised crime, much like identity theft or hacking. We are really working in three main ways to try to tackle that problem. The first is around our policies and our enforcement approaches. As you may have seen, we have been evolving



HOUSE OF COMMONS

our policies over many years to tackle financial services issues in terms of our advertising. Most recently, we launched a financial services certification. Any advertiser wanting to target a UK user with a financial services ad has to be FCA authorised and has to pass identity checks before it can run that ad.

We have also continued to update our policies, for example our unreliable claims policy, so that advertisers cannot claim to be offering a return that seems unreasonable or unfeasible. That was done in consultation with the FCA. That is the first area in terms of policies.

Q269 **Chair:** On that point, when the FCA gave evidence to this Committee it pointed out that it was having to spend a lot of money—it said £600,000 in the last year—advertising with Google in order to warn people not to engage with these scam advertisements. How does that square with everybody being FCA approved, as you put it?

Amanda Storey: We work very closely with the FCA. We have done for the last several years. I have met with Charles Randell and Nikhil personally a number of times. We have offered ad credits to them as part of helping them with their user awareness.

Q270 **Chair:** Does that cover the whole £600,000 that they have spent?

Amanda Storey: We have offered them £1.5 million at this point.

Q271 **Chair:** Does that cover everything they have spent in regard to having to warn people about adverts that your company is taking and posting online?

Amanda Storey: We are in discussions with them about exactly what they will need, and we are running that alongside all our own education efforts and things like our Digital Garage programme.

Q272 **Chair:** Sorry, my question was very specific. The £1.5 million is a commitment, I take it.

Amanda Storey: Yes.

Q273 **Chair:** Once that is paid, does that mean the FCA will be sitting there feeling that it has been reimbursed for all the advertising that it has had to purchase to clamp down on fraudulent adverts on Google?

Amanda Storey: We have offered them these credits, and they are discussing with us whether they can make use of those. We have also offered credits to—

Chair: Are you in a negotiation where you have basically said, “Yes, we will reimburse everything you have spent in order to clamp down on a problem that is due to the advertisers on our site”? Does that £1.5 million cover all of that or is there more? Might the FCA say, “Actually, £1.5 million is very useful, thank you, but there is a lot more that we have spent in addition to that”?



HOUSE OF COMMONS

Amanda Storey: We absolutely agree that user education is an important part of tackling this problem, and we are investing in that education ourselves as well as with others and with the FCA.

Q274 **Chair:** That is not answering my question, with great respect. It is a very simple question. Does the money that you have offered the FCA cover all that it has spent on advertising to try to stop people engaging with these fraudulent ads that are appearing on the site?

Amanda Storey: My understanding is that they are using a multitude of ways of educating users. They are using social influencers as well as ads, and the £1.5 million—

Q275 **Chair:** I am still not getting a direct answer to the question, I am afraid. Could you write to the Committee to answer that very specific question? It may be that you do not know the answer to it.

Amanda Storey: We can absolutely follow up in writing with more details.

Chair: I am sorry; I interrupted. Please continue with what you were telling us.

Amanda Storey: No, it is a totally fair question. I was talking about the policies we have put in place. We also have scaled enforcement that we do. For example, in 2020, we took down over 3 billion bad ads, including 123 million financial services-related ads globally. We are doing policy changes to keep pace with the threats that we see to users and we are also taking enforcement decisions at scale to protect users on our platforms. That is the first area.

The second is collaboration. We are working very closely with the FCA, as we have mentioned. We are also working very closely with the online fraud steering group in partnership with the Home Office, DCMS and others. I personally have joined the board of Stop Scams UK—we were the first tech company to do so—to collaborate with banks and telcos on how we can address this issue and share signals to get ahead of the threats we see to users. We feel that collaboration is a really important part of this.

Then the third and final piece is user education. Your question is entirely fair. User education is really important here, and we see multiple avenues there. We have offered £1.5 million in credits. We are running what we call Digital Garage sessions, including with many of your constituencies, to educate people about online safety, and Be Internet Legends, which is targeted at children, related to online safety. We are really trying to make sure users have awareness of the threats that are out there and the right information to make informed decisions, as well as the policy, enforcement and collaboration points that I mentioned.

Q276 **Chair:** I know I am like a dog with a bone on this, but can I come back to it? I might have misunderstood. Is the £1.5 million you referred to in



HOUSE OF COMMONS

credits for advertising for the FCA? It is not a refund on the money that it has spent to date.

Amanda Storey: That is correct. It is in ad credits.

Q277 **Chair:** On the question of the £600,000 that it has spent in the last year, what is the situation on that? This Committee feels that it should be refunded to the FCA. Can I ask what your opinion is on that?

Amanda Storey: I am very happy to follow up in writing. We are in discussions with the FCA about that point and making sure that it has the support it needs.

Q278 **Chair:** If you would, that would be great. Would somebody else like to come in on my original question? I am happy if anyone else wants to come in on this point. What is your assessment of what is happening on your particular platforms and what steps are you taking to deal with the problems? Nobody is stepping forward. Perhaps I can ask Gaon if he would be brave enough to step into the ring, please.

Gaon Hart: Yes, of course. I am happy to assist. Amazon, as everyone is aware, is a retail store online. We have 1.9 million small and medium-sized enterprises that work through us, and they total globally about £3.5 billion worth of export sales. That is about 65,000 in the UK alone. The essence is that this makes us a target for fraudsters. That is why last year we spent \$700 million in order to protect our stores from fraud and abuse and to protect customers.

More importantly, we also employ 10,000 independent and committed experts to think about the future, to live in the future and to start thinking about not only the fraud of today but also the frauds that are potentially going to happen—

Q279 **Chair:** Could you sum up the top three frauds of today that relate to Amazon for us?

Gaon Hart: LexisNexis reports a 94% increase, particularly recently, in scams. These are scams in which people are pretending to be from Amazon, HMRC or the Post Office, as you will have seen.

We have three broad types of scams. You are talking about the customer support scams that we see, where someone pretends to be from Amazon or from another organisation, and sits there and tries to get access to somebody's details. The others are recruitment scams and brushing. There is then retail fraud, which is fraud on the site by either sellers or buyers either not sending the goods or, alternatively, not paying for the goods, essentially.

For the overwhelming majority of the increase in fraud, which is generally being reported by Action Fraud and the US Better Business Bureau, the single biggest vector is the scams that do not touch the store; they occur off-store, using Amazon's or other people's names. Even then, we try to assist in four clear ways. We take the lifecycle of a fraud. The first



HOUSE OF COMMONS

requirement is that someone must gain access. We have in-depth verification procedures. We managed to block and prevent over 6 million people regarding accounts last year when we felt there was some form of abuse. We also blocked over 10 billion listings that may have been as a result of fraud and abuse. We have also updated our verification processes recently. Access is one area we are really focusing on.

The second area of importance is that you must somehow make changes. You must divert the money to yourself. If you have taken over somebody else's account somehow, you do not want the money that you are defrauding from people to go to them. Every day we scan over 5 billion potential changes to listing pages to try to ensure that there is no fraud and abuse resulting from that activity.

We also scan 45 million pieces of customer feedback, because often somebody will say, "This is not very good; I did not receive the product," etc.

Q280 Chair: This is quite detailed, but very helpful. What is the penalty for you as a business if you end up with lots of this dodgy stuff on your site? There is a reputational risk—we all understand that—but, other than that, how does it hurt your business if this stuff goes on there?

Gaon Hart: The first thing to say is that Amazon is the most customer-centric company in the world. That is how it is maintained. If customer trust is lost, they simply will not revisit our site. Our stores are there for people to come, purchase and feel comfortable.

One of the key areas, therefore, is that there is no commercial incentive for us to allow or to permit this in any way, which is why we spent over \$700 million and why, more importantly, we have effective technological capabilities such as IP geolocators, natural language processing, visual text and smishing comparisons against templates. Depending on the circumstances, we use a combination of human intelligence and really intelligence-led tools that can assist in this.

Q281 Chair: Are they all effective? How effective are they?

Gaon Hart: As I say, we estimate that it has stopped 10 billion potential listings from bad actors.

Q282 Chair: How many does it not stop? What proportion of those trying to abuse the site is it not picking up?

Gaon Hart: It is difficult to say. The stage of the process where we are at is the front line of the defence against fraud, essentially. We provide the purchase capability. We then have our tools that, as I have discussed, try to protect the site. They work really effectively, as do, more importantly, the people who are there to update them. The fraudsters we are facing are agile and dynamic. It is sophisticated individuals and organised crime doing this.



HOUSE OF COMMONS

As we say, we need to live in the future. We need to think about not only the frauds of today but those of tomorrow. In that respect, though, in the architecture of the UK's counter-fraud controls, we are at the beginning stage. We are on the front line of defence. Therefore, you will find that we will see only suspected frauds. Part of our role in the process is to ensure that we pass these to law enforcement, to the banks and to other organisations in order to analyse this better and find out whether it is or is not a fraud.

Q283 Chair: Thank you very much. That is very helpful. Can I just throw this over to the whole panel? The Online Safety Bill is in draft form at the moment. You will be very aware that there is a big debate about whether within the scope of that Bill should be online advertising, so that your sites would have a duty and responsibility to ensure that fraudsters and scammers are not operating, probably with penalties in the event that some get through.

To most people, to the general public, that seems like an eminently sensible idea in order to hold you truly to account. Is there anyone on the panel who believes that is the wrong way to go? If so, could you explain why, please? If you are silent on the point, I will assume you think it is a good idea.

Amanda Storey: We have not waited for regulation. The changes we have made are making a difference to the prevalence of scams on our services. We recognise that online advertising is already subject to the CAP code and the DCMS online advertising review is coming up. We hope to engage in that process constructively.

In terms of the Online Safety Bill itself, it is designed for user-generated content. When you look at the traits of user-generated content versus scams, they are quite different. With user-generated content, someone looking at policy and a piece of content could make a pretty clear decision about whether that content is violative. With a scam, you are looking at one signal. That cannot necessarily tell you whether it is a scam; you need to look at the actor, the behaviour and the piece of content itself to ultimately make a decision about whether it is a scam.

The techniques for user-generated content and for scams are quite different. Therefore, the Online Safety Bill is not necessarily targeted in the way that it would need to be to be efficient at tackling online scams. That needs to be considered.

Q284 Chair: If you took where you are at the moment, which I understand is that voluntarily you are insisting that all investment advertisements are FCA approved, for want of an expression, why would it be wrong, given that is your position, to have some kind of penalty there when you let people through who did not meet that criterion that you have set?

Amanda Storey: Again, we have not waited for regulation. We have done everything that we can do to make sure scams are not appearing to users.



Q285 **Chair:** In the event that you let people through who should not be getting through—I do not know whether that happens or not—would it not be fair and reasonable for there to be a penalty in that circumstance?

Amanda Storey: We absolutely bear responsibility for what appears on our sites, and we make sure every day that we are protecting users. That is what my team does. We have over 20,000 people around the world who are making sure we keep users of our products safe. We are investing over £1 billion a year in technologies and humans to enforce at scale and keep users safe.

Q286 **Chair:** I am running a little short on time, but I am just going to ask Allison this question of refunds to the FCA for moneys it has spent with you, trying to dissuade people from engaging with fraudulent activity on your site. Where are you on reimbursing the FCA for those costs, please?

Allison Lucas: We provide a significant amount of in-kind support to the FCA, and other UK regulators and consumer groups, to help to raise the profile of consumer awareness campaigns. We have done this with the FCA and the ASA, so we have already done this. I also understand from earlier testimony today that the FCA will be running a consumer awareness digital campaign, and we are looking forward to supporting that as well.

Q287 **Chair:** My question was very specifically on the moneys that the FCA has spent with Facebook on trying to dissuade people from engaging with inappropriate investment content on your site. Will you be refunding that money to the FCA?

Allison Lucas: I am not aware of that detail, but I am happy to take it back.

Chair: If you could write to the Committee, I would be very grateful. Will, I am so sorry I did not get to you, but that may be a relief—who knows?

Q288 **Julian Knight:** I wish to declare an interest: I am the chair of the new and advanced technologies APPG. Amanda, I was quite struck by your answer to the Chair there. To paraphrase what you said, this is too much like hard work. Do you not owe a duty of care to your users?

Amanda Storey: We absolutely do. We have a huge responsibility to make sure that users are protected on our services. That is literally what my team does every day: making sure users are protected, with humans and machines working together to deal with the scale of the challenge that we see. Then we have humans to deal with the complexity and nuance of individual content decisions that might be more borderline.

Q289 **Julian Knight:** Why can we not have the duty of care that is a part of the online harms legislation apply to non-user-generated content that is fraudulent?

Amanda Storey: There are differences in user-generated content. The Online Safety Bill talks about the automated means that can be used to



tackle that content. We absolutely think that is the right approach for user-generated content. Automated means alone, though, are not going to be sufficient to tackle scams. It really does require the kind of sustained and strong collaboration that we have started to engage in with the online fraud steering group and with Stop Scams UK. You have to have the signals from all sorts of players across the value chain to identify something as a scam. We think the mechanism is different.

Q290 Julian Knight: You just mentioned collaboration. This is a really interesting point. If you want to persuade legislators not to bring about legislation that applies to your industries, and to use softer or lighter-touch regulation, you four huge players who are with us today need to show us that you are working together.

I have a very simple question for you, Amanda. How much information do you share with one another on the types and incidences of economic crime on your platforms?

Amanda Storey: The online fraud steering group is a collaboration among many members. Equally, we were the first tech company to join Stop Scams UK, but others are now joining as well, which I am really pleased to see. This is definitely a less mature collaboration area than some. When we look at something like violent extremism or child safety, there are much more—

Q291 Julian Knight: With respect, it sounds like a talking shop. What about data? What about information? What about credit card details? What about flags to say that this particular post is a potentially fraudulent post? Gaon, what do you think? Are you sharing your information and data with Facebook, Google and eBay?

Gaon Hart: The key is that, as I said before, we are at the forefront; we are at the start of this process. We have suspected fraudulent data. The banks and law enforcement have the final decision.

Q292 Julian Knight: Are you sharing data? With respect, are you sharing data?

Gaon Hart: We share SARs, suspicious activity reports, which is information on suspected fraudsters. We send those to the FCA and we do share those.

Q293 Julian Knight: You share that with the FCA. Do you share with Google? Do you share with Facebook? Do you share with eBay—yes or no?

Gaon Hart: We share with law enforcement.

Q294 Julian Knight: You do not, then. Fine, that is okay. We understand. Allison, on the same question, when you gather information on your platform and you see flags to indicate that someone is a potential fraudster, do you share that information with Google? Do you share that information with eBay? Do you share that information with Amazon—yes or no?



Allison Lucas: It is the same response. We share with law enforcement when we are asked to provide it.

Q295 **Julian Knight:** Will, are the words “we share it with law enforcement” about to come from your lips?

Will Semple: We are very keen and proactive. We work with a lot of law enforcement not just in the US but in the UK and across Europe. However, if I might bring some extra colour to the conversation, eBay has a very proactive response to fraudulent activities and cybercrime activities that happen off our platform. On many occasions, we reach out directly to the platform that may be hosting the advertisement or the page that is causing the problem.

Q296 **Julian Knight:** You mean phishing scams using eBay. You are talking about phishing scams, effectively. You are saying that you may reach out to, let us say, Gmail or Hotmail, which may be hosting those particular scams. Is that right?

Will Semple: It could be customer support scams, phishing or account takeover. We very proactively reach out and regularly engage with the main registrars who are providing the hosting of the actual domains to take down these activities that lead to fraud occurring.

Q297 **Julian Knight:** What is the response from them? Does it always end with, for example, an account being closing down, etc.? I do understand your position, because eBay is probably the most exposed in many respects to this type of phishing and other types of scam. When you send your email to Google or you say to it, “We have seen this suspicious activity; there is an account here that is a Gmail account,” what does it do? Does it always take it down?

Will Semple: The direct answer to that is not every single time, but the vast majority of times. That is leading very much into a key direction that we need in order to tackle this type of fraud and cybercrime. As has been mentioned so far today, there is very good collaboration within the broader ecosystem not just between—

Q298 **Julian Knight:** Will, thank you for that. I am very short on time so I am going to move on, because I want to drill down. Thank you for that contribution, though.

Allison, why is it that you do not share this data between the platforms? I would have thought that it would have been entirely logical at least for Google, as a company that draws in a huge amount of advertising spend, to co-operate and say, “Hold on. This advertiser that you are taking here is dodgy.”

I have some experience in this. I used to work in national newspapers many moons ago. I can tell you that they shared that type of information on a regular basis in order to stop scams within their newspapers. Why are you not doing that? Why are you not effectively co-operating with Google in order to focus on these scams and get them taken down?



HOUSE OF COMMONS

Allison Lucas: The concern that we would have would be a privacy concern. Anything that we can share in a privacy-safe way we will with the online fraud steering group, but otherwise we would have—

Q299 **Julian Knight:** Are you more concerned about fraudsters' privacy than people being robbed of their life savings?

Allison Lucas: No, we are concerned about privacy concerns for our users.

Q300 **Julian Knight:** These users are fraudsters, and they are trying to make people's lives a misery. I cannot see why, frankly, it is not beholden on you to put in place systems in order to flag this across your platforms. You are asking us not to regulate you. Therefore, you need to show that you are doing everything in self-regulation. I do not really buy privacy, frankly, as remotely sustainable in this context.

Is it not just the fact that you are also interested in retaining data? Effectively, you all have these walls in place because data is money, power and position in the industry.

Allison Lucas: I appreciate your comments and concerns. We also agree that there is a responsibility for safety and to prevent harmful content on our platforms. We have committed to doing all of this. We have committed to our users through our policies, our enforcement practices, our collaboration with the FCA and the ASA, and these tech groups. We take responsibility, and we take a variety of approaches to address all of these concerns. Whether it is through proactive enforcement or whether it is reactive, we work very closely with the FCA and the ASA.

Q301 **Julian Knight:** Amanda, the two largest advertising companies in the world are you and Facebook. The scale of online advertising is huge. Alphabet has a higher turnover each year than the economy of Holland, for instance. Why is it that you are not sharing this fundamental data when it comes to trying to track down these individuals, close them down and ensure they do not appear on your platforms?

Amanda Storey: We are absolutely taking all of the signals that we can get access to. We have automated the FCA's alert list; we use the Advertising Standards Authority's scam alert list, and we have done since 2020; we take alerts from the police. We have acted on those in a very rapid way, and we have even trained them on how to make sure they are getting those signals to us quickly. We want to work with banks, telcos and other tech players to make sure we are integrating signals from them to deal with—

Q302 **Julian Knight:** You are not working with Facebook, apart from these talking shops.

Amanda Storey: We absolutely have experience of working with Facebook, for example through GIFCT in the violent extremism space. We would love to see similar signal sharing in the scam space as well.



Chair: The points that Julian has raised are very good points about data transfer between your businesses. Could I ask all four witnesses to write to the Committee to set out the data you do transfer, to whom you transfer it—you have mentioned the FCA—and the reasons why it might be that you are not currently transferring data of the type that Julian has described between your businesses and other similar businesses, please?

Q303 **Alison Thewliss:** If I could start with Gaon and ask a little bit about what you are doing to prevent fraud and scams, Amazon does not sell financial services directly, but there is a page within your advertising site that encourages financial services advertising. Nothing on that page says anything about advertisements for financial services products having to be authorised by the FCA. Why not?

Gaon Hart: We have a policy that requires authorisation by the FCA. We enforce that policy within our verification processes. We also have prohibitions and security to make sure that our customers are not faced with high-risk products, short-term loans etc. We do ensure and have processes to ensure that they are compliant.

Q304 **Alison Thewliss:** Why is it not on your site?

Gaon Hart: I am not fully conversant as to where something is or whether it is on a page or not. It is clear in our policy. There is a policy that relates to it. We have a unique position when it comes to advertising, because we are the advertiser, the DSP and SSP intermediary, and also the publisher on the other side. That gives us quite an opportunity to ensure that advertising is compliant with our product requirements and is vetted properly. We have verification processes, and we are certified members of TAG in relation to malware and privacy. We undertake quite a lot of assurances, controls and processes in order to protect in advertising terms.

Q305 **Alison Thewliss:** That does not quite answer the question. Why it is not there? You have the page that says “financial services advertising”. It says, “How can Amazon Advertising fit into your financial services marketing strategy? Learn about the advertising solutions we can offer your financial services company, whether it’s insurance, banking, brokerage, or tax”, but there is nothing there about having that FCA approval. Why is that not there? It should be up there at the front to say, “We want to encourage good businesses that are legitimate to come here”. Why would you not put that up at the top?

Gaon Hart: As far as I can see, the reality is this. Do we ensure that our customers are protected from malware, malvertising and fraudulent advertising? That is the key. It is having the processes and the verification elements behind in order to make sure. Once somebody comes through and asks to provide those adverts—I accept fully that it is not there, although I do not know that particular policy—the essence is for us to ensure that they are compliant with all the requirements. That is



HOUSE OF COMMONS

one of the key things we focus on. We focus on protection and protecting the customers.

Q306 **Alison Thewliss:** Would there not be soft element of deterrence to put that at the front?

Gaon Hart: I am happy to take that back and talk to the internal team, but the essence is about the protections that we provide.

Q307 **Alison Thewliss:** Can I turn to Amanda to follow up on some of the issues that have been raised by colleagues about FCA-approved ads? Do you still allow adverts to run before the advertisers have been verified?

Amanda Storey: No, no one can run before they have been verified.

Q308 **Alison Thewliss:** When did that change?

Amanda Storey: We launched that policy in early September, but we have been working on different types of verification for businesses and for individuals for many months at this point. We have been taking advice from the FCA and others on how to do that effectively.

Q309 **Alison Thewliss:** What was the date in early September?

Amanda Storey: I believe it launched on 6 September. We had to give notification to advertisers in advance and then we changed that policy on the 6th.

Q310 **Alison Thewliss:** So it is too early to say whether that has had much of an impact.

Amanda Storey: From what I have seen, it is having an impact and we are confident that it will.

Q311 **Alison Thewliss:** Can I ask what the read-across to YouTube and other Google services is?

Amanda Storey: Yes, the ad policy is exactly consistent. The process is consistent. The FCA checks that we have put in place for ads running on Google also apply to YouTube.

Sitting suspended for a Division in the House.

On resuming—

Q312 **Alison Thewliss:** I want to ask about what more Google is doing to ensure that services such as YouTube are not being used to promote investment scams and other frauds. Specifically, what are you doing about user-generated content, which may mislead people? Obviously, financial advice is a regulated industry.

Amanda Storey: On YouTube, we have community guidelines that prevent any illegal behaviour, and then we also require YouTube creators to disclose if they are paid to promote something. We are trying to provide as much transparency to the user as possible and regulate the



behaviour that is happening, as well as making sure that users have access to helpful, high-quality information.

Q313 **Alison Thewliss:** How much of that is proactive and how much do you rely on people complaining about having seen something online?

Amanda Storey: Our detection is both proactive and reactive. We have the ability for users to flag things that they consider to be harmful or concerning to us directly within the product, both for YouTube ads and ads on other Google services. We also have proactive detection mechanisms. We have 20,000 people around the world who are doing content moderation every day, and a raft of very sophisticated preventive techniques. When you look at something like Gmail, you can see the scale of that. We prevent over 100 million phishing attempts every day and 15 billion spam emails every day.

Q314 **Alison Thewliss:** If somebody were to subscribe to somebody's channel on YouTube to follow their financial advice and to end up losing a lot of money out of that, is that then your fault for not having prevented that?

Amanda Storey: We absolutely take responsibility for the quality of the content on our services and for user safety on our services. We work very hard every day to moderate both the content and the actors operating across our services, which is why we take action at the ad or video level as well as at the channel or account level.

Q315 **Alison Thewliss:** Which? has found that even when platform users do report fake and fraudulent content it is not guaranteed that the content will be removed. Its research from last year—I appreciate that things have changed in that year, although from the start of September it might be too soon—found that a third of victims of a scam, which began from a fake and fraudulent advert, who reported it to Google said that the ad was not taken down.

Amanda Storey: That is really surprising to me. Certainly, the changes we have made to verification and that gate before anyone is allowed to advertise are really important steps in making sure that no one even has access to the system to distribute fraudulent ads.

Q316 **Alison Thewliss:** I am sure Which? would be happy to speak to you further on that. Turning to Allison Lucas, I wanted to ask about the extent to which you protect users from adverts and products for firms not authorised by the FCA.

Allison Lucas: We have a number of ways that we do this. We do it both proactively and reactively. I would love to talk about the different ways that we do this. I would like to start by saying that we feel our greatest responsibility is ensuring the safety of our users. Because of that, we have a global team of about 40,000 people, about half of whom do content moderation. Largely, and this is in every single area, we do this through product design, artificial intelligence and policy safety, all with user safety at the heart of what we do.



HOUSE OF COMMONS

What we do is, as Amanda said, both proactive and reactive using policies and technology. If I can just talk about how we do this both proactively and reactively, in our unpaid content, so what we call organic, we have the combination of proactive and reactive. We do this proactively by removing violating content. We do it through artificial intelligence. There is certain content that we remove through content moderation teams. Users can also remove content that they do not want to see, if they think it is irrelevant or inappropriate, and reports can also come through third parties like the FCA, which is also onboarded to a channel where it reports this to us. We also have proactive warnings. Users are given a warning when they are talking to someone who we think might be a scammer. They are sent a message when we see, perhaps, abusive language. We have that as well.

On the advertising side, we have ads that are reviewed prior to publishing. This is a combination of signals, ad characteristics and other information to detect potential policy violations. That is on the review side. Knowing that this is not perfect and that some ads may get through, we also have ads that can be reviewed after something is published, and those ads can be taken down as well after the fact. They also have an ability to be reported, so those are taken down after the fact as well.

Q317 **Allison Thewliss:** Thank you very much. That is useful. Can I ask a wee bit more about your approach to user-generated content, where that may be fraudulent as well? There are people out there giving financial advice when they are not qualified to do so. What would be in place to stop me giving duff financial advice and asking for investment on Instagram?

Allison Lucas: We do have policies. If you are talking about yourself, we do have policies against fraud and deception. If you are just discussing it, it may not rise to the level of a policy violation. If you were actually encouraging it, it would be taken down. There are policies in place for that.

Q318 **Allison Thewliss:** As a constituency MP, my experience of trying to get things taken down off Instagram on behalf of my constituents has not been good, I can say.

I am curious. Looking at Instagram, on the way to the vote and back, I looked up the hashtag "investment". It brings up tonnes of pictures about where to invest your money, which sectors to invest in and lots of stuff about cryptocurrency. All of those are sitting on Instagram right now, including one that is around property investment advice and learning how to build stocks and build wealth. It has a picture of Google's headquarters on it as well, which is nice for Google. Perhaps some chat between you later might be appropriate on that. The person who posted that has 643,000 followers. How do I know that that person is giving good advice?

Allison Lucas: I cannot speak to the specific content, but, if there is an indication of any sort of investment scam, something that promises



HOUSE OF COMMONS

guaranteed results, that would be violative content and we would remove it under the policy. Any user is able to report content, which we can then look at and take down if it violates the policy.

Q319 **Alison Thewliss:** Yes, but there is so much of that out there. There are 19.8 million posts with the hashtag “investment” on there. It feels as though nothing is really going to be possible there, given the scale of that issue.

Allison Lucas: If the content does violate, we would take it down.

Q320 **Alison Thewliss:** How many of those posts are you likely to take down from 19.8 million?

Allison Lucas: I do not know the specific numbers. You are allowed to discuss investments, and that does not violate our policy.

Q321 **Alison Thewliss:** Yes, but financial advice is a regulated area.

Allison Lucas: Yes, but you are allowed to discuss the content. This is not just for online content. If you are online, you can also be doing this across the board. You are allowed to discuss this offline as well. We do not regulate discussing these areas.

Q322 **Alison Thewliss:** Yes, but, if we are discussing where to invest your money, “where to oversight your money” sounds like advice to me. If I do not know very much about that, if I am seeing that on Instagram, if it is being shared among my friendship group, how do I know I can trust that? I do not.

Allison Lucas: Again, if it takes the step to tell you to go do something—to promote it—we would take action on it.

Q323 **Alison Thewliss:** Moving on slightly to some of the activity on Facebook, can I ask how you regulate closed Facebook groups?

Allison Lucas: For pages and groups, we have pages, groups and events policies as well.

Q324 **Alison Thewliss:** You may be aware—I would be interested in what response has come from this—that in May “File on 4” reported that Facebook had been used in the establishment of 48,000 mini-umbrella companies, in which people were recruited via Facebook for a tax avoidance and evasion scheme that the QC Jolyon Maugham has described as “industrial-scale tax abuse”. Why is that allowed to be perpetuated on your platforms?

Allison Lucas: I am not aware of this particular issue, but I am happy to take it back and take a look at the issue you are specifically referring to.

Q325 **Alison Thewliss:** This was essentially a fraud against Companies House. People were being recruited to be company directors via this website in order to avoid tax in the UK. Why is that allowed to be happening on a closed Facebook group? Why are these not being shut down?



HOUSE OF COMMONS

Allison Lucas: If it rose to the level of a policy violation, we would remove it. I am happy to take a look at the issue.

Q326 **Alison Thewliss:** Is tax avoidance not a policy violation?

Allison Lucas: If it was any sort of discussion of an investment, it would be allowed. If it rose to fraud and deception under our policies, it would not.

Chair: On that last point about the tax avoidance group, perhaps the team here could liaise with you, Allison, just to make sure you are very clear as to the group that is being referred to. You could write to the Committee with answers to the questions that have been asked. Thank you very much.

Q327 **Harriett Baldwin:** Allison, I am going to carry on asking you some questions about Instagram. It started off as a platform for sharing photos and now you have these very massive influencers who are often pumping or alluding to investments in cryptocurrencies and all sorts of unregulated areas. Does that worry you? If it does, what steps is your organisation taking?

Allison Lucas: It is a similar issue. We do look at these. The overriding aim is to keep our users safe. For the same reason that we allow our users to discuss and share advice on trading and investment, users, whether they are paid by a brand or not, are allowed to talk about knowledge, tips or anything. If it rises to an investment scam, if it promises a guaranteed return or any sort of promise of investment, it would violate our policies.

We do not always know whether a relationship exists between a brand and an influencer. If one does, they have to use a branded content tool. We make sure that that is available and we ask that they disclose the relationship between the brand and the influencer so that the nature of the post is clear.

Q328 **Harriett Baldwin:** Do they have to disclose if they already own that particular financial asset before they pump it to all their Instagram followers?

Allison Lucas: No, they have to disclose their relationship to the brand. They have to disclose that it is an advertisement.

Q329 **Harriett Baldwin:** They would not have to say it is an advertisement for something that they already hold or have holdings in.

Allison Lucas: They just have to disclose their relationship to the brand.

Q330 **Harriett Baldwin:** Would you consider increasing the disclosure that you require your platform users to use on financial promotions?

Allison Lucas: We would consider anything that is required in order to make clear there is a relationship.



HOUSE OF COMMONS

Q331 **Harriett Baldwin:** Could you tell me what revenues your firm is enjoying from content providers in the financial arena that have subsequently proved to be fraudulent?

Allison Lucas: I do not have those figures. I am sorry.

Q332 **Harriett Baldwin:** You are one of the largest global data companies. Are you trying to say that you do not have those figures?

Allison Lucas: I do not have those figures, no.

Q333 **Harriett Baldwin:** Would you be able to follow up by providing us with those figures?

Allison Lucas: I do not have a breakdown of the figures by vertical.

Q334 **Harriett Baldwin:** Would you be able to ask the financial team to provide you with that information and to share it with the Committee?

Allison Lucas: I can come back on that.

Q335 **Harriett Baldwin:** Thank you. I have the same question to Google, really. As I understand it, from 6 September you have started this new process. That means the FCA has to have already authorised a financial product before it goes on the platform and might be seen here in the UK. Is that right?

Amanda Storey: That is correct. Anyone trying to advertise to a UK user with a financial services ad has to be on the FCA authorised list.

Q336 **Harriett Baldwin:** That is since 6 September.

Amanda Storey: That is correct.

Q337 **Harriett Baldwin:** Prior to 6 September, can you share with the Committee what sort of revenues Google was enjoying from that activity?

Amanda Storey: The change that we made on 6 September is just the latest change in a long history of trying to make sure we are keeping users safe on the platform. We introduced identity verification and business operations verification back in March of this year. We have introduced policy changes over multiple years to make sure users are kept safe.

In terms of a specific calculation of revenue from financial services ads that might subsequently turn out to be fraudulent, it is a really fair question, but there are some serious challenges in calculating that. You have both a false negative and a false positive problem here. We do not always know that something was a scam. That is why we have put this gate in place, because we recognise that it is the only way for us to ensure that these advertisers are legitimate.

Q338 **Harriett Baldwin:** When you put the gate in place, you must have gone up through management and explained what you were going to do. Often that will mean you have had to provide some sort of financial



HOUSE OF COMMONS

quantification of the impact of that change. What was that financial quantification within Google?

Amanda Storey: We are always trying to make sure that we balance creating friction for bad actors and allowing legitimate advertisers to efficiently access customers. We absolutely look at the size of the—

Q339 **Harriett Baldwin:** Can you share with the Committee what that amount was?

Amanda Storey: I could follow up in writing and see what we can share there. I would go back, though, to how you have a false positive and a false negative challenge here. We do not always know that something was a scam ad. That is one of the challenges. We also sometimes have advertisers that we think might be fraudulent, which we take down, and then they subsequently provide the identity verification, such that they are proven to be legitimate and can then run ads. We do have that challenge in doing any calculation.

Q340 **Harriett Baldwin:** On 6 September you must have had to take down quite a lot of content, mustn't you, as a result of this change?

Amanda Storey: Yes.

Q341 **Harriett Baldwin:** Are you able to quantify what the value of the revenue stream was for the content pages that you took down on that date when the policy changed?

Amanda Storey: I could follow up and provide more information.

Q342 **Harriett Baldwin:** Do you have a hunch as to how much it would have been?

Amanda Storey: I do not, I am afraid.

Q343 **Harriett Baldwin:** Could you put it in context for the £1.5 million of free credit that you are effectively offering the FCA instead of the cash that it has spent with you on putting stuff on your platform?

Amanda Storey: What I can share is that there are some categories of financial services advertisers that are not FCA authorised, which we have had to just prevent at this point. For example, the FCA does not authorise crypto, some SME lenders or gold. These are all categories that we have now prohibited, because they are not on the FCA authorisation list.

Q344 **Harriett Baldwin:** You can no longer get any crypto content on Google.

Amanda Storey: Crypto ads, yes.

Q345 **Harriett Baldwin:** That is in the UK.

Amanda Storey: That is anyone targeting a UK user, yes.

Q346 **Harriett Baldwin:** What about on YouTube? There are quite a lot of videos up there that you can watch about that.



HOUSE OF COMMONS

Amanda Storey: Yes, the same authorisation applies to YouTube ads as well.

Q347 **Harriett Baldwin:** This was from 6 September. Am I right in thinking that this is quite a meaningful change in terms of the impact it will have on Google's revenue from this kind of activity?

Amanda Storey: Yes, this was a really significant change for us.

Q348 **Harriett Baldwin:** But you cannot quantify for the Committee how significant—just ballpark—at this point.

Amanda Storey: I do not have the numbers to hand, but I am happy to follow up and see what we can provide in writing.

Q349 **Harriett Baldwin:** Can I bring in Amazon and eBay and ask similar sorts of questions? What is your revenue stream from this? We heard today from UK Finance that an extra 30% was scammed out of UK consumers last year. How does it compare to that?

Will Semple: From eBay's perspective, we have had a longstanding policy of selling goods, not financial services. We do not permit the sale of any financial services, cryptocurrencies or investments on our platform at all.

Q350 **Harriett Baldwin:** So it is zero. It has never had any revenue or top-line impact on your business.

Will Semple: Not as far as I am aware or that I have been advised by our financial team at this time, no.

Gaon Hart: Similarly, we are a retail store. It is online, but it is a retail store. To be honest, one of the key things that we point to is an external organisation called Confiant, which has estimated the amount of malvertising on stores. It has estimated that the average generally across companies is around 0.11%. Ours is at around about 0.01%. We know this is not a significant impact for our customers. Any impact whatsoever must be avoided, and we focus quite a lot on restricting this, but it is not a major challenge for us in this respect.

Q351 **Harriett Baldwin:** Amanda, all the Google content targeting UK users is now off your platform.

Amanda Storey: All ads, yes.

Q352 **Harriett Baldwin:** All paid-for ads

Amanda Storey: Correct, yes.

Q353 **Harriett Baldwin:** You can say that with complete confidence. There should not be any content left that targets UK consumers. It was actually quite easy to find them and to get rid of them, then.

Amanda Storey: Yes, this change is very significant for us. We are confident that it will dramatically reduce the risk that a user is exposed to



HOUSE OF COMMONS

a scam. Again, it is the latest change in a raft of changes that we have made to try to address this issue. We will need to continue innovating. The work here is never going to be done. These are sophisticated organised criminals, who will continue to innovate and find ways around the systems that are being put in place, so we need to continue to innovate as well.

Q354 Harriett Baldwin: You also must have quite a lot of information that you could share with law enforcement about the people who have been paying for this content. Are you doing that?

Amanda Storey: We do, absolutely. We have a dedicated team engaging with law enforcement. We have actually done training with the College of Policing about how to best inform us about frauds that they identify so we can act on those very quickly. We provide information back about the actions we have taken.

Harriett Baldwin: It is worth repeating just how much money our constituents are losing to this kind of activity. We are voting today on the London Capital & Finance compensation, which the taxpayer is having to cough up. Thank you very much for your evidence.

Q355 Siobhain McDonagh: Amanda and Allison, I want to ask you about fraud and young people. Often we consider that this is for older people who do not know their way around social media. Only by doing events in my constituency about crime and online crime have I become aware of how big it is.

I understand that Instagram, Allison, is owned by Facebook. Can you tell us what you do about money mules, when you have anonymous people on your site who are advertising to young people on the issue of money mules?

Allison Lucas: It is the same as it would be for anything. Our policies cover both anonymous and any other advertisers. We have the same approach as for anything. Our policies cover fraud and deception. We will take the same approach that we would take in any other way.

Q356 Siobhain McDonagh: How many staff do you have on the issue of money mules in the UK?

Allison Lucas: Our policies and our enforcement are global. The reason is that we want to cover across languages and we want to cover this globally. We do not actually take an approach that is UK-specific.

Q357 Siobhain McDonagh: How many people do you have internationally?

Allison Lucas: We have 40,000 people who cover safety. About half of those cover content moderation, but it is 40,000.

Q358 Siobhain McDonagh: How many people do you have on Instagram?

Allison Lucas: It covers both Facebook and Instagram.



Q359 **Siobhain McDonagh:** How many users do you have?

Allison Lucas: How many users do we have?

Q360 **Siobhain McDonagh:** Yes, internationally. You have 40,000 people who look at this issue.

Allison Lucas: That is across all of our users.

Q361 **Siobhain McDonagh:** How many of them are there?

Allison Lucas: I cannot recall the exact number, but this is for all of our content moderation.

Q362 **Siobhain McDonagh:** When parents talk to me, they tell me that they tell Instagram about the problem, and the sites and the adverts do not come down. How long would it normally take you to react to somebody's complaint?

Allison Lucas: It depends on the piece of content, but it should usually be a very, very quick process. There is a way for users to look at a piece of content, and for organic content or unpaid content you could actually look at any piece. There is an area in the top corner of a piece of content with what we call the three dots, and you pull down and you can actually report that piece of content. It is a very, very quick process. I just want to make sure that we are not conflating the unpaid piece with the advertising piece. You can do that for an organic or an unpaid piece of content, as well as any advertising piece as well.

In terms of users, just to take a step back, we have about 3 billion users. Just so you understand, we have 40,000 people looking at safety across our platform of about 3 billion.

Q363 **Siobhain McDonagh:** What proactive education do you do for young Instagram users? As I am sure you will know, if you are a young person who gets involved in this and you lose your bank account, it is extraordinarily difficult to get another legitimate high street bank to take you on, which has huge implications for you. I recently had a 14-year-old girl whose account was taken away because she followed advice about money-muling on Instagram.

Allison Lucas: We do a significant amount to work and educate customers and consumers. We support the FCA's proposals through our online fraud steering group. We have been doing education. We have significant educational campaigns about the platforms and throughout the internet.

Q364 **Siobhain McDonagh:** What does "significant" mean?

Allison Lucas: We provide monetary support, and we work with the steering group as well as the FCA to educate consumers.

Q365 **Siobhain McDonagh:** Amanda from Google, the BBC's "Panorama" has a programme next week in which it has found somebody who is selling



HOUSE OF COMMONS

guides on how to defraud people and how to commit fraud online. This young man has a number of YouTube videos about him. How big do you think the problem is on YouTube?

Amanda Storey: We have very strict policies on YouTube. We have scale enforcement techniques that we use, with machine learning as well as human moderators, to make sure we are addressing any problems that we see. Fraud of this kind is organised crime. The scammers are incredibly sophisticated, so we have to keep pace with that level of innovation.

Q366 **Siobhain McDonagh:** You would think that child trust funds were simple and straightforward. There are 55,000 people each month who become 18 and therefore have access to their money, which should be a really good thing. Unfortunately, this is another huge area on Instagram where young people are being defrauded of their funds, yet you have very few adverts about it. UK Finance's biggest campaign is Take Five—To Stop Fraud. I understand that that is not very promoted on Instagram. Why would that be?

Allison Lucas: We do have a number of awareness campaigns. We do work with Take Five. We also have a help centre article to help spot scammers on Instagram. As I said, we do have pretty significant promotion for this. I will take that back and I will see if there are other ways that we can promote it, but we have a pretty good user awareness campaign, as I said, in addition to the help centre articles that we have on Instagram.

Q367 **Siobhain McDonagh:** Is the issue for everybody that the problem is increasing at such a rate in such volume that you really cannot keep up with it? You are not really prepared to put in the huge investment that it would take to resolve these problems. As Harriet said, it is £4 million a day just in this country; it is £754 million in the first six months of this year, which is an increase of 30%, with 70% of fraud online. Is it that you just cannot manage it? What would Facebook and Instagram say?

Allison Lucas: We have every intent to do as much as we can to address this. We provide in-kind support. We are working with the fraud steering group. Like I said, we have every intention of increasing support as the problem increases as well.

Q368 **Siobhain McDonagh:** Amanda, I have been to your events at a primary school in my constituency. I have been out with your bus. They are great initiatives, but they are tiny in comparison to the volume of the problem. Is it that you just cannot invest enough to stay on top of it?

Amanda Storey: These criminals will always continue to innovate. That is why our approaches have to evolve too. The latest change that we have put in place in terms of this gate for only FCA-authorized advertisers is a really important step to keep pace with what we see going on, and we are confident it will dramatically reduce the risk that our users are exposed to scams.



HOUSE OF COMMONS

I agree with the comments that Charles Randell has made about the blending of enforcement and education. Both of those are important, and that is why we invest in the sorts of education that you have mentioned as well as funding others to do education.

Q369 Dame Angela Eagle: There is a new Online Safety Bill going through the House of Commons at the moment. It deals mainly with issues of anti-terrorism and child sexual abuse, which is another terrible feature of the social media platforms that you have all pioneered—a bad side to what is going on.

Would you agree, Amanda Storey, that we should incorporate fraud and economic crime in the regulations that we are putting on our statute book so we can try to bear down on this problem?

Amanda Storey: The Online Safety Bill is really world leading. The UK is leading the way in defining what online safety can look like. It is a bill that is very targeted at user-generated content. That is a fundamentally different type of content for which a different type of enforcement is required than for something like a scam. The scam journeys weave online and offline; they weave internationally. You need information about the actor, the behaviour and the content to make a decision about whether something is a scam.

The large-scale automated enforcement that the OSB describes is not necessarily an appropriate mechanism for scams. That is why we have put in place things like the certification scheme to have that gate upfront, because we believe that is the most effective method of reducing the risk.

Q370 Dame Angela Eagle: We could extend the scope of the Online Safety Bill to include things like that. As a company, would you be happy to see fraud included in this kind of regulation? I accept the point that you have made about user-generated content, but it is possible to regulate in other areas too. Would you be happy with that?

Amanda Storey: There is an interesting international example here. When you look at something like the Digital Services Act that the EU is considering at the moment, there is a section in that related to trusted flaggers. This goes to your points, Julian, about flag sharing. That could be a really interesting mechanism to encourage further sharing. It is something that we do extensively already in the violent extremism space and the child safety space. We have very mature organisations like GIFCT and the Technology Coalition, which do extensive flag sharing to make sure we can all be taking much more preventive action.

Q371 Dame Angela Eagle: Allison Lucas, what would Facebook's view be of extending the regulation in the Online Safety Bill, which is currently going through the House of Commons, to economic crime and fraud?

Allison Lucas: I would like to preface this by saying that my UK public policy team is a bit closer to this Bill than I am. I would also say that Facebook shares the Government's ambition to make the UK the safest



place to be online. This Bill is largely positive. But fraud is incredibly complex. If fraud were introduced, Ofcom would have to grapple with a lot of these issues. It would be a challenge to include fraud within this Bill. The user journey touches a number of touchpoints, both online and offline, before the fraud even takes place, so including it with this Bill comes with a lot of different challenges.

Q372 Dame Angela Eagle: I understand that, but I suppose the harms that are being increasingly done by the all-pervasive nature of the platforms that you run are becoming so great that there is going to be some form of regulation. It will possibly be global if it carries on, but meanwhile each individual country is going to try to do something about it.

I suppose people could cynically think that Facebook does not want to do an awful lot, because you are making so much money from advertising and you can just carry on coining that in until more heavy regulatory action is taken. Would it not be better to welcome regulation?

Allison Lucas: We do welcome regulation significantly. We are always calling for regulation in this space. We are calling for regulation of Facebook all the time. We also feel like expert stakeholders are already looking to address fraud, whether it is through the fraud action plan, the DCMS commitment to using the online advertising programme to look at paid-for advertising, and things like the fraud steering group. We feel like this is already being covered in a number of other ways.

In addition, absent regulation, we are already covering this and looking at it through our policies and through our enforcement mechanisms.

Q373 Dame Angela Eagle: Is enough happening, given the huge increase in online fraud that we saw both prior to the lockdowns and especially during the pandemic lockdowns? There has been a huge increase in this kind of activity. The harms are increasing, and the scams are increasing. As a regulatory authority, we seem to be miles behind all of that. The victims are my constituents and the constituents of everybody else on this Committee.

Allison Lucas: I feel that we can always be doing more. We are constantly looking to increase our efforts and increase our enforcement. We can always do more, but this may not be the venue to do that.

Q374 Dame Angela Eagle: Do you have a strategy for combating fraud that you are happy with? You have said that you could always do more. Why do you not do more?

Allison Lucas: We do. We do it through the proactive and reactive measures that we have, whether it is through the increase in our enforcement that I talked about earlier, or the consumer policy channel in which we work closely with groups like the FCA and the ASA.

Q375 Dame Angela Eagle: Does Amazon have anything to say about these kinds of scams? I know it does not affect you as much as it does the



HOUSE OF COMMONS

Googles and Facebooks of this world.

Gaon Hart: Yes, but anything that affects our customers affects us significantly. I appreciate that the Online Safety Bill is a hotly debated topic. It is right that it covers user-generated content and that it covers the predatory harms that it is aimed at. These are terrible to victims. I have seen it as a former prosecutor. As a cybercrime champion, I have spoken to multiple victims in the past and seen the devastation that these cause.

The question has to be about what the right methodology is. What is going to be effective in reducing fraud and reducing such elements? Where the Online Safety Bill is looking at predatory harms, currently there is not sufficient or much legislation or many regulatory requirements in that area. It is right that it beefs it up.

In the areas of fraud and corruption, there is quite considerable legislation. There is FCA regulation. This provides a quite protective layer. The question is whether this is a matter where legislation can really make a difference or whether what we are facing is a technological war, a smart war, in which the bad actors are sophisticated criminals. What will really make the difference from our perspective is not so much greater legislation in this area, but rather greater partnership and, as was explained, a greater breaking down of the segmentation of information, so that, if a bank has identified a bad actor, for example, it shares that with others and, if the FCA has information, it shares that with others.

Q376 **Dame Angela Eagle:** The FCA certainly thinks that the Online Safety Bill should be expanded to include fraud. It has told us that.

Gaon Hart: I appreciate that, but nobody has explained to my satisfaction whether that is the best methodology and whether that is going to move the dial. That is what we need to do. We need to make a change. That is what Amazon is focused on. What can reduce and protect customers and society as a whole?

If you look at the international models, everybody is starting to move to the extent where it is the three major players that have the information and the capability that should be co-operating together more: it is law enforcement and Government, civil society and companies.

That is what we are trying to do through the online fraud steering group. We have already made one significant step in the fact that five companies—it is approximately five—have offered \$1 million of free advertising for the Take Five campaign. The aim of that is to have consistency, so that, when you go into a bank, you see a consistent message. Equally, we have to think about how we can move the dial and what the best methodology is.

Q377 **Dame Angela Eagle:** What this online safety group does is not in the public domain. Is anybody able to tell us here and now what its aims actually are?



HOUSE OF COMMONS

Amanda Storey: I do not sit on the online fraud steering group myself. I do sit on the Stop Scams UK board. Just last week, I was presenting at the board meeting about the experience we have had from flag sharing in other areas and how that could be a really interesting way for the group to progress in terms of the telcos, banks and tech companies, which are now following our lead and joining up, sharing more flags to get ahead of this issue.

In relation to your questions on regulation, we are not waiting for regulation. We want to protect our users; we want to keep them safe on our platforms. That is why we are putting in place the new policies and the new enforcement mechanisms that we have, as well as doing things like integrating and automating the FCA's alert list.

When we look at the numbers from that alert list, the vast majority of the flags that we are receiving from the FCA we have never had live on our platform or have already taken action on. The residual are the flags that we want so that we can take action and protect users.

Q378 **Dame Angela Eagle:** Is that the aim of the group? Do you have any targets that you can share with us?

Amanda Storey: Do you mean the Stop Scams UK group?

Q379 **Dame Angela Eagle:** No, this working group.

Amanda Storey: I am afraid I am not on the online fraud steering group myself. Another representative from Google is. Perhaps someone else could speak to that.

Q380 **Dame Angela Eagle:** Is it possible for all of you to write to us to explain what you think this group can achieve and what it is aiming to achieve? It is quite shadowy from our point of view. If it is anti-fraud, clearly it might have to be shadowy, but I think you could share it with us.

Amanda Storey: Absolutely, we would be happy to.

Q381 **Julie Marson:** Staying with you, Amanda, it might seem a while ago now but in the original conversation you had with the Chair about the FCA, the £600,000 and you offering £1.5 million, you referred to negotiations with the FCA. If the FCA comes to you and says, "This is what we need," why is it a negotiation?

Amanda Storey: I am not sure I used the word "negotiation". It is definitely a discussion. We want them to take up these ad credits that we have offered. We want to be part of educating users. That is why we run our own programmes, and we have offered money also to UK Finance for the Take Five campaign, as well as ad credits to others who want to invest in educating users about online risks.

Q382 **Julie Marson:** If the FCA says, "This is what we need financially," it is not a negotiation. Effectively, you will give it what it needs.



Amanda Storey: We have offered the ad credits. We are happy to stand beside that offer and we are discussing what more we could do with them.

Q383 **Julie Marson:** I am going to ask each of the panellists to give us a bit more detail about how you work with Government Departments in countering economic crime. Which Departments do you work with and how do you work with them? Maybe I can stay with you, Amanda, to start with.

Amanda Storey: We have dedicated teams who work with law enforcement around the world, including in the UK. There are a few avenues of how we work with them. We are looking for alerts from them about illegal activity that we can then take action on. We also respond to lawful requests for information. We provide transparency about all of that broken down to the authority level and the country level, and we have done so for over 10 years now because we believe that transparency is important.

We also do education. We want to make sure that people know how to use our systems and send alerts to us. That is a very streamlined process. We have done dedicated education with the College of Policing, for example, and the City of London Police.

In terms of collaboration, many have talked about the existing collaborations in this space. Those are important in terms of tackling this issue. They include the online fraud steering group, Stop Scams UK and the integration with the Advertising Standards Authority and the FCA alert list.

Gaon Hart: The key is these partnerships. We have a very good relationship with law enforcement, we feel. We feel they are very approachable. We also provide evidence and details about suspected bad actors. Not only that, but we also have investigation teams that work with them in order to explain and help to educate them as to how our processes work and where the weaknesses are. That goes on in order to ensure we get better enforcement. That is the key, so that we can start increasing the deterrent.

There are other areas that we work in. We are on the online fraud steering group. That steering group sits under the fraud justice group. That is quite an important element. One of the three co-chairs is Graeme Biggar, who is the director of the National Economic Crime Centre. The approach is to try to get banks to start collaborating with different types of organisations and to open it up following the JMLIT model, which has been quite successful in the money-laundering field.

As a result of this, we have also provided our internal experts to that group. For example, afterwards we have had requests for conversations with those experts, because they can provide that technical information. These are complicated areas. Importantly, it is about your abilities, your



HOUSE OF COMMONS

passion and your dedicated experts, because this is a technology question. It is about looking and thinking, as we say, in the future.

We are talking and discussing regularly with the NCSC, with the Home Office—we recently provided a presentation—and with civil society, Which? etc., to explain how our processes work. That is the area that we need to start to work on. I completely agree with the previous form of questioning. We need to start to break down those segmented information barriers.

Q384 Julie Marson: There is a lot of talk about discussions, collaborations and so on. You mentioned Graeme Biggar. He has said that online platforms are enablers of fraud. You have not really convinced him in that respect, have you, when he says that?

Gaon Hart: As Amazon, we do not recognise that in any way. We are a retail store online. The fact is that we consider ourselves to be at the front line of defence for our customers. We are not an enabler. We are there putting in place protections. As I say, we spent \$700 million just last year. We have 10,000 people working to try to protect customers and everyone, and to give them trust in our stores. Amazon is the first line of defence, rather than an enabler.

Allison Lucas: We have a number of channels and are in collaboration with a number of groups. I should preface this by saying that this is also more our UK public policy team's domain, but I will represent them as I can. We have the FCA relationship and the regular engagement. The purpose of that is for the FCA to share trends and for it to be able to report content through our consumer policy channel. I understand that it works pretty well.

We also engage with the Advertising Standards Authority on a number of issues and initiatives like the scam ad alert system, which we have been a part of since it started. We also have the online fraud steering group, and then we have law enforcement. Not only do we respond to legal requests from law enforcement, but we have a good relationship with the dedicated card and payment crime unit at the City of London Police. That has existed since 2019, and it is managed by trust and safety law enforcement outreach in London. Those are the different avenues that we have. We work with the dedicated card and payment crime unit as well.

Q385 Julie Marson: What about central Government Departments like the Home Office and the Treasury, getting into the economic crime plan?

Allison Lucas: We work with those as well. We are always responding to and working with law enforcement.

Q386 Julie Marson: How do you work with the Home Office and the Treasury?

Allison Lucas: I believe I will have to take that back, actually. I do not have the exact details.



Q387 **Julie Marson:** Perhaps I could ask Amanda about that. What about central Government Departments like the Home Office or the Treasury, and feeding into the economic crime plan? How does that work?

Amanda Storey: The online fraud steering group—I am sorry to keep coming back to that example—includes the Home Office, DCMS and the National Economic Crime Centre. We do have routes into all those Government entities. We work with Government and law enforcement in a very active way. We have dedicated teams that do that.

Q388 **Julie Marson:** Amanda, what message would you like this Committee to send to Government about the best way of preventing online scams?

Amanda Storey: There are three main things here. Certification is really important, so considering the definitive list of good actors that everyone can use and refer to. I know the Committee has discussed previously the perimeter of the FCA's certification and whether that needs to be expanded. That would be interesting to consider. Collaboration is also really important. We have talked extensively about that here also. Finally, it is about making sure that there are education campaigns so that users are aware of the risks online and able to respond to the information they are seeing.

Q389 **Julie Marson:** Perhaps I could go back to Allison with the same question. What would your message be to Government via this Committee?

Allison Lucas: It is a very similar answer. We are always happy to collaborate and discuss best practices. I know our UK public policy team is doing the same and actively engaging. We would love to have engagement with tech companies on defining best practices and principles. To go back to an earlier conversation, sharing data in a privacy-safe way is a challenge for industry and other sectors, and one that we would love to continue working on. The tech industry's Take Five initiative is a good example of this.

Q390 **Julie Marson:** I do not know, Will, if you want to add anything to that discussion.

Will Semple: Yes, eBay recognises that economic crime, cybercrime and online fraud are transnational problems, and we respond to them in a global way. There are lots of committees and groups that we participate in, but, if I may, I would speak to our engagement on a day-to-day basis on the front line with many agencies. We engage with the FBI and the Secret Service in the US; with the NCA and the Met Police in the UK; and with Europol and individual police units across Europe and Asia. We actively pursue fraudsters and the organised crime that is committed on our platform.

We take a very proactive and very lean-in approach to pursuing and removing these types of bad actors not just from our marketplace but from the environment in total.



Q391 Rushanara Ali: Good afternoon. I wanted to talk some more about regulation, but ahead of that I have a few follow-ups. Gaon Hart, you were saying that fraud is incredibly complex. We have heard a lot about educating the public, but you as an expert are talking about the complexity of it. Are all of you, as companies, engaged in what could be described as a cop-out by using that as your answer to some of the questions we have heard today?

Just as we have seen after the financial crisis, with banks being expected to know their customers, should you not be proactively paying for the cost of the fraud that each of your companies may be engaged in? We have seen some examples. All of us recognise the powerful positive benefits of the internet and the opportunities it has presented. There is no question of that. We need to make sure we clean up the act where it is going badly wrong. Otherwise, it poisons the environment in which our citizens have to operate.

Gaon Hart: There are a number of parts to that question. The essence for us is that we would challenge the fact that we enable fraud. We are the front line; we are the first line of defence for fraud. That is where we focus our proactive controls.

You are absolutely right about education and awareness. It is one of the elements that have demonstrated that there is an increase in reporting, we hope, coming out. One of the things that I love about Amazon's guidance, tools and the things we provide is that we add to the Take Five message that says, "Watch out. There are frauds. Be careful." We have a number of guides—we have given some examples to the clerk—that give people a chance to empower themselves before they become a victim.

Q392 Rushanara Ali: I have heard what you have said about the positives. Where there are areas of improvement, what is your view? If your company is not responsible for fraud that then takes place on top of what you have done, in terms of meeting the gaps, is there a case for regulators to fine your companies, all of which inadvertently, shall we say, enable fraud to happen on your platforms, as a parallel to the things that happened through, for instance, the de-risking of banks? The banks cleaned up their act, because they knew they were going to be fined hundreds of millions of pounds, and in some cases in fact much more.

Gaon Hart: They did. Taking de-risking as an example, it led to over de-risking.

Rushanara Ali: Precisely, yes. That is my point.

Gaon Hart: The fines led the other way.

Q393 Rushanara Ali: This is why I am raising it. I raised some of the concerns around de-risking. You are talking about self-regulation and doing all the things that you are doing. Is it not time that, as institutions, you stepped up so that that did not happen? None of us wants to see inappropriate regulation, but we do not want excuses and we do not want our



HOUSE OF COMMONS

constituents continuing to suffer. That is where we are so far, I am afraid.

The reality is that Google has made a mockery of the regulator of this country by expecting the regulator to take down fraudulent stuff from the site and to pay for it. Today you are talking about entering into dialogue and discussion, yet giving no straight answers as to why on earth Google is not paying back the money that the regulator had to pay in order to take stuff off your site that you should be responsible for.

Amanda Storey: We are not waiting for regulation. We want to keep users safe on our platform. We find it abhorrent that anyone is falling victim to a scam. We have taken extensive measures to make sure that users are safe when they use—

Q394 **Rushanara Ali:** I suppose this is what I am saying. If the FCA had to pay for a bank's failures, we would be up in arms. I am a big fan of Google; we are all dependent on Google. Lots of good things happen in our constituencies because of it. There is no question of that, but your company has put the FCA, the regulator of this country, in an embarrassing situation. In effect, what has happened is a joke. The regulator has had to pay you in order to take down stuff that you should not have put on there in the first place.

Should a legal requirement now be placed on each of you where you are proactively required to make sure this stuff never sees the light of day? Is that not where the regulation should be?

Amanda Storey: We have collaborated very closely with the FCA over the last two years. I have met with Charles and Nikhil myself multiple times.

Q395 **Rushanara Ali:** Should it be enshrined in law? Otherwise we are relying on your goodwill, embarrassment, bad media coverage and reputational damage for you to possibly get there. It has taken a long time.

Amanda Storey: We are not shy of taking action at all. We have put in place the verification scheme against the Financial Conduct Authority's verification list. To give you another example of where we take extreme measures to protect user safety, when Covid was first playing out we banned all Covid-related adverts across all our services. We got extensive criticism from businesses and from Governments for that move, but we did not feel we could serve Covid ads at that stage in a safe way, so we took all of them down. We are not shy of taking those sorts of actions to make sure that users are safe. That is why we have put in place the certification scheme that we have and why we have taken multiple other actions.

Q396 **Rushanara Ali:** From an industry-wide perspective, there will be variances in what is happening, who is doing what, who is doing good work and who is not. Notwithstanding all the working groups that you have established, what we need is outcomes.

I will give you a parallel example of counter-terrorism and online hate. A



HOUSE OF COMMONS

few years back, I had a constituency experience where Facebook and other social media platforms were being used by extremist groups. The then Government intervened, because the police were having to take down and report stuff that was online that was extremely harmful and being used to groom young people to become extremists. The same has happened with religious extremism and far-right extremism. Lots of progress has been made there. Can we learn from that?

It seems to me that, because financial fraud is often seen as victimless in terms of the narrative—we have heard lots of people talk about it in that way, but it is not victimless—the same level of effort is not being put into financial fraud and what is being hosted by social media sites and the sites that many of you host. That is what needs to happen, so it is automatically done and you are putting the investment in because you are legally required to do so. Otherwise, we are going to get varying practices.

You have heard from Alison Thewliss about the number of things that are there that people have to navigate, which is almost impossible because the public is bombarded with stuff. If a company cannot get a grip, how do you expect our constituents to get a grip or get a handle on any of this? Feel free to come in, but would anyone else like to come in on this point? Maybe it is time for Facebook to come in.

Allison Lucas: I do not have too much to add. Again, it is a public policy point, but we would call for content regulation. We do want to see proportionate regulation in this space.

Q397 **Rushanara Ali:** You would agree with content regulation.

Allison Lucas: We would agree with content regulation. We are waiting to see what the outcome of the Online Safety Bill is. We agree with proportionate regulation in this matter.

Q398 **Rushanara Ali:** Can I ask others whether there should be content regulation and responsibility enshrined in law for preventing content from appearing on your sites? Would anyone else like to come in on that or add anything on that?

Amanda Storey: I would just comment again that we are not waiting for regulation.

Q399 **Rushanara Ali:** That is not the question, with respect. Would you agree with legislation that requires you to? We appreciate what you are doing proactively, but some would argue that, because there has been a lot of attention in this Committee on what you have done and how you have made a mockery of the FCA, you have put in those changes ahead of this Committee. We welcome it, but it is public and media pressure that often leads companies to take action, so what is the answer to the question?

Amanda Storey: The change that we made with the FCA certification—

Q400 **Rushanara Ali:** No, sorry, would you support regulation? That is the



HOUSE OF COMMONS

question that Allison was able to answer in a straightforward way. Could you answer that question? Do you support regulation to have online platforms taking legal responsibility to prevent content appearing on your site?

Amanda Storey: It is, ultimately, in our view, up to the Government to decide.

Q401 **Rushanara Ali:** But the question is what your view is as a company. You are the company, with respect, that has acted in a, frankly, appalling way, where the regulator has had to pay you to take stuff off, when you have been responsible for hosting material on your sites that are fraudulent.

Amanda Storey: What the FCA has been doing is education, using our services to contact users.

Q402 **Rushanara Ali:** That is not my question, with respect. My question was whether you support regulation to address this particular point. You are not answering it—yes or no?

Amanda Storey: We share your concern.

Q403 **Rushanara Ali:** Why do you not answer the question? It sounds like it is a no. It is absolutely a perfectly respectful position, if it is a no, but we need to know the answer.

Amanda Storey: We do not think that the Online Safety Bill is the right vehicle for regulation. We are happy to engage in the online advertising—

Q404 **Rushanara Ali:** I just have one more question for Allison. This is related to other aspects. When we talk about fraud and financial crime, we need to look at where we are coming from, and that is why I am drawing parallels with what has happened with terrorism and far-right crime and hate. There has been good work but, unfortunately, very serious things have had to happen before work has been done to mitigate damage to institutions like Facebook. When it started, Facebook was a positive force for good. Many of us use Facebook for our own work. Sadly, it has become synonymous with very negative things too, including fake news, hate crime and hosting stuff around terrorism.

In 2018, the UN fact-finding mission's investigation by Yanghee Lee into the genocide committed by Myanmar against Rohingya Muslims concluded that Facebook played a "determining role" in that genocide. In her words, Facebook turned out to be "not what it originally intended" and "has now turned into a beast". We need to make sure that regulation is established in such a way that these platforms, which are generally a force for good, are not used for hate crime or inciting violence and, in this case, contributing to genocide. That is the level of damage, at its worst, that platforms can do.

What should be done at an international level to make sure that Facebook is never associated with genocide and other crimes?



Allison Lucas: We make clear in our standards that we do not allow any criminal organisations to have a presence on Facebook. We remove all praise, support and representations of organisations when we become aware of it, and we are continuing to invest in artificial intelligence to help improve this enforcement. We are continuing to look at it and to invest in this type of enforcement, to make sure that that does not happen.

Q405 **Rushanara Ali:** How much, in monetary terms, are you investing? We have heard from Amazon about how much it has invested. You mentioned some numbers. Could you just clarify how much you are investing in preventing fraud, as well as hate crime, extremism and genocide, in your case?

Allison Lucas: I do not have a specific number for that. As I referenced earlier, we have 40,000 people who are working on safety and security. We have invested \$13 billion in teams and technology in this area since 2016.

Q406 **Anthony Browne:** As you may know, I used to be chief executive of the British Bankers' Association, and one of my responsibilities was overseeing all the anti-fraud activities in the banking sector, working with the Home Office, the FCA, the Bank of England and the banks themselves. At that time, I must say, I always thought that, on a whole range of measures, the technology and social media industries were way behind and on a journey. We see that you are on a journey, but various comparisons have been made with the banking industry.

I will ask my first questions to Google. I am sorry if some of this was covered earlier, because I missed the first half of the session. If their customers are victims of fraud, banks have a policy for compensating them. They do not always compensate, if the customer is deemed to have been negligent or grossly negligent. For run-of-the-mill fraud, they will compensate the customers, even if the banks did nothing wrong. Will you compensate customers who are victims of fraud that is advertised by you when you put them in touch with fraudsters?

Amanda Storey: We have a responsibility to deliver a safe experience on our services, and we are investing heavily to make sure that we keep that experience safe.

Q407 **Anthony Browne:** If somebody is put in touch with a fraudster through Google, and they lose money as a result, will you compensate the customer 100%? Do you have processes for that?

Amanda Storey: We are working hard to make sure that we are never in a position where a user needs to be compensated.

Q408 **Anthony Browne:** Can you answer the question? Have you ever compensated any customer who has lost money through fraud via Google?

Amanda Storey: We have not.



HOUSE OF COMMONS

Q409 **Anthony Browne:** Will you look at compensating any customers who lose money through fraud via Google, in the way that the banking industry does?

Amanda Storey: We are working to get to a position where no one needs to be compensated.

Q410 **Anthony Browne:** That is taken as a given. Hopefully you eliminate fraud 100%, but it is unlikely. Fraudsters are very imaginative. If you do not eliminate fraud 100% and there are still people who are victims of fraud and lose money as a result of Google's activities, will you compensate them?

Amanda Storey: That is not something that we have in place at the moment.

Q411 **Anthony Browne:** Will you look at putting that in place in a way that the banking industry has? I can guarantee that you are on a journey where it will be in place at some point, and it is far better, reputationally, for you as an industry to be ahead of the curve, rather than being behind the curve by enabling fraud and refusing to compensate. You are one of the world's richest companies.

Amanda Storey: We absolutely want to keep pace with the criminals and the way that they are behaving.

Q412 **Anthony Browne:** But you are refusing to compensate people who lose money as a result of your activities, which you make profits on.

Amanda Storey: I would be really happy to follow up in writing and explain some of our thinking.

Q413 **Anthony Browne:** Why are you refusing to compensate customers who lose money as a result of Google?

Amanda Storey: As I said, we are working to do everything we can to make sure no one needs to be compensated.

Q414 **Anthony Browne:** I am going to ask the same question of Facebook. Have you ever compensated any customer who has lost money as a result of fraud through Facebook advertising?

Allison Lucas: I also do not have the answer to that.

Anthony Browne: You do not know whether you have compensated any customers for losses that they have suffered as a result of your advertising.

Allison Lucas: I can also say that we are investing money to tackle the underlying issues and to prevent the ads from running in the first place.

Q415 **Anthony Browne:** Can you answer the question? Have you ever compensated any customers for losses that they have incurred as a result of advertising on Facebook?



HOUSE OF COMMONS

Allison Lucas: I do not know that we have.

Q416 **Anthony Browne:** Should you not know that you have? It seems extraordinary that you do not even know your own company's policy on whether you compensate customers for loss as a result of fraud that you facilitate.

Allison Lucas: We are also committed to solving this bigger picture.

Q417 **Anthony Browne:** Everyone is committed to solving fraud, but you are unlikely to eliminate it 100%, because fraudsters are incredibly imaginative and agile, and there will still be people losing money—often livelihoods—as a result of advertising that Facebook, Google and others facilitate. You are refusing to compensate customers or you do not do it at the moment. Will you look at compensating customers for losses they incur as a result of your advertising?

Allison Lucas: I understand that, and I would still say that we will look at solving the bigger picture.

Q418 **Anthony Browne:** You are avoiding the question, so you are saying that you refuse to look at whether you should compensate customers for fraud in a way that the financial services industry does.

Allison Lucas: I will take that back as well.

Q419 **Anthony Browne:** I do not quite understand what "I will take that back" means, but you are refusing to commit to it. The reason I mention it is that taking financial responsibility for fraud is incredibly important in terms of creating internal incentives within companies. Banks know their fraud loss rates, because they compensate customers for fraud. They know how much it costs them and they have an internal financial incentive to reduce fraud as much as possible, so that they do not have to pay out for those losses. As companies, you have none of those internal financial incentives, and you profit from fraud. You profit from advertising fraud and you do not suffer any of the losses. Do you agree with that analysis? I am asking you first, Allison, and then Amanda.

Allison Lucas: I am sorry. I would say that we do not want this content on the platform. It makes a bad experience for our users and our advertisers, so we are incentivised to eliminate this.

Q420 **Anthony Browne:** You are profit-making companies, which is absolutely fine and I am all in favour of it. You have internal managers who have profit and loss accounts. Unless they suffer losses, and unless fraud costs you money, however much your goodwill and your concerns about your broader reputation, you have no internal financial incentive to tackle it.

Allison Lucas: We do not.

Q421 **Anthony Browne:** So you are quite happy having no internal financial incentive to tackle fraud. Coming to Google and the same question, unless you compensate customers for fraud, you profit from fraud and do



HOUSE OF COMMONS

not lose from it. You have no internal financial incentive to tackle fraud and it is basically a PR exercise. Is that right?

Amanda Storey: No, absolutely not. Bad ads are very bad for business. Our business and our ads ecosystem absolutely depend on trust.

Q422 **Anthony Browne:** But you make money out of bad ads. You profit from them, and you profit from getting the regulator to advertise against the adverts that you promote.

Amanda Storey: We have taken measures to shut down parts of financial services advertising where we do not believe we can operate safely. For example, with introducing the FCA's certification process, we have turned off multiple advertisers in the crypto and SME lending space.

Q423 **Anthony Browne:** I get all that and that is great. I take that for granted, and I have been heavily involved with a lot of this in the financial services industry, but you are not taking financial responsibility for the fraud that you facilitate. When I said that you are behind the curve on this, the message to you and your senior managers is that you need to be ahead of the curve and to take financial responsibility for the fraud that you profit from and facilitate, which you will carry on facilitating, however much good work you do—and you do good work. That is the journey that you need to be on internally. You need to have internal senior management discussions about it, because, until you do that, no one will take you seriously.

I am sorry if this was covered earlier. On the £600,000 that the FCA paid you to advertise to warn your customers of the fraudsters that you were profiting from promoting, I assume that you do not dispute that figure.

Amanda Storey: No, we do not dispute that figure.

Q424 **Anthony Browne:** I assume you do not think it is good or right that the regulator had to give you money to advertise against the fraudsters that you were profiting from. That is not right, is it?

Amanda Storey: That is why we have offered £1.5 million in ads credits to the FCA, yes.

Q425 **Anthony Browne:** Another question was whether you have done that. That is good. At least you have taken responsibility for that.

I want to ask Amazon the same question. I know that fraud is very different with you, but would you compensate your customers who are victims of fraud?

Gaon Hart: Yes, absolutely. As you can imagine, as the most customer-centric organisation, we have an A-Z guarantee. It is not just fraud. If you order a product and it does not arrive—

Anthony Browne: You have a very good returns policy.

Gaon Hart: It is not only returns.



HOUSE OF COMMONS

Q426 **Anthony Browne:** No, but if people have problems with it, or if it is not what it says it is, you compensate for that.

Gaon Hart: We will compensate, and we do the same or similar, depending on the circumstances, for sellers.

Chair: That brings us to the end of this session, which may be a relief to some of our witnesses. Who knows? Can I thank all four of you for appearing before us? Your platforms and what you do are hugely important to every one of us. Everyone on this Committee, at one time or another—probably daily—uses the services that you provide, and it is probably only fair to say that we should not forget that they give a lot of people a lot of satisfaction, as well as being a bit of a Wild West situation when it comes to the issues we have been discussing, in some cases leading to very dark places indeed for many of our constituents, so it is of huge concern to us.

Everyone around this table wants the same thing, and I have no doubt that all four of our witnesses and the companies they represent also want to have a safe space for people to operate. None of us wants to see people scammed or be subject to fraud. We cannot overestimate the challenge that there is, given both the volume of what is going on out there and the entrepreneurial skill, if that is the right term, with which some of these dreadful people unfortunately operate.

The Committee is not saying that your companies are doing nothing at all. You have spoken at great length about a lot of things that you have been doing, with a lot of people and money being put into trying to address these kinds of issues. Amanda made the point about FCA-authorized advertisements and the change that came in earlier this month, which should be welcome. You have spoken about the policies you are operating to and the work you are doing in terms of screening, the use of AI and so on. But that is not the same as saying that enough is being done.

We have heard today from Julian in particular about this issue of data sharing, to make sure that, across the various businesses, yours and others, you are as effective as you can be at working together to get on top of this problem. We have heard from Allison and others about how effective this screening really is. There seemed to be plenty of anecdotal evidence, at least, and lots of evidence in the numbers that many problems are getting through the systems you are deploying.

Anthony made a fair point about financial responsibility, which is there in the banking sector, and is a great driver of change and getting on top of these issues, but seems to me to be largely absent in the businesses that you operate.

Then there is this issue of legislation and regulation. No Government want to have to be stepping in and regulating marketplaces. We want you to be as free as you can be, but there are certain things that we, as a society, cannot tolerate. Therefore, as you will have surmised from the questions from this Committee, it is the Committee's view that the



HOUSE OF COMMONS

Government should be legislating to bring advertising and fraud into scope with the Online Safety Bill.

At various points during the discussion today, you very kindly said that you will write to the Committee, and the Committee will write to you to remind you of what it is that you have committed to. Equally, we might have some additional questions to ask, and we would very much appreciate a written response to that when we send it through to you.

Could I conclude by thanking you once again for coming and appearing before us?