Fraud Act 2006 and Digital Fraud

Corrected oral evidence: Fraud Act 2006 and digital fraud

Monday 23 May 2022

3.40 pm

Watch the meeting

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

Evidence Session No. 13 Virtual Hearing Questions 135 - 145

Examination of witnesses

Elizabeth Kanter, Graham Pullan and Philip Milton.

The Chair: Welcome to this afternoon's Select Committee session on the Fraud Act 2006 and digital fraud. A transcript of the meeting will be taken and published on the committee's website. You will have the opportunity to make corrections to that transcript where necessary.

We are very pleased this afternoon to be joined by three representatives from social media platforms: Elizabeth Kanter, director of government affairs and public policy manager at TikTok; Graham Pullan, CEO of Fluttr; and Philip Milton, public policy manager at Meta. Without further ado, Lord Vaux will ask the first question.

Q135 **Lord Vaux of Harrowden:** Good afternoon, everyone. Social media is obviously known to be a key factor in the recent increases in digital fraud. Perhaps you could tell us what preventive steps you take actively to stop fraud before it happens on your platforms and a little bit on how that has changed over time as methods of committing fraud have evolved. Perhaps we could start with Philip Milton.

Philip Milton: Absolutely. Thank you for the question. I would like to start by thanking the committee for inviting us. This is a really important area and one that is important to us. The safety and security of our users is our absolute number one priority. Without our users, our platforms cease to exist; it is as simple as that. Fraud puts that at risk and degrades the experience for our users. Even if they do not necessarily fall victim to fraud, the very presence of it degrades users' experience, and it

makes it an unattractive place for advertisers to use as well. It really is the number one priority for the organisation.

Fraud is a rapidly changing area and we have to ensure that our detective systems are up to date to combat it. To give you a quick idea, we have invested about £13 billion in this area to date. We have 40,000 people across the organisation working on it; 20,000 are directly involved in reviewing content. We have learned a few things over the years, so we have learned to focus on bad actors rather than on individual pieces of content.

To give you an example, we focus on fake accounts, in particular. We find that, more often than not, bad actors tend to use fake accounts when they engage in fraud. In the last quarter, we removed 1.6 billion fake accounts from our platforms, and 99.7% of those were taken down before users reported them to us, so we have become very good at finding fake accounts and removing them. We think that is a really important effort.

Our aim is always to catch the fraud before it reaches users. We know that we will not always be able to do that. As I said, it is a fast-moving space; it is difficult to catch everything, so we make it easy for users to report things to us when we do not catch things. We then ingest that information and feed it into our AI systems and our machine learning, hopefully to better catch that fraud the next time round.

We carry both ads and organic content on our platforms. I will break down very, very quickly what we do on each. For ads, we have a set of strict advertising policies, which set out what you can and cannot do on our platforms, on Facebook and Instagram. Those ads prohibit deceptive or misleading practices; that is what catches the fraud definition. We run an ad review process that checks all ads that run on our platforms against those policies. We remove any ads that fall foul of those policies.

In organic content, we run a mix of proactive detection and reactive action. We have AI detection that focuses on behaviour over content. The reason for that is that we have learned over time that fraudsters change their actions depending on what we do. They can quite easily change a picture or a phrase being used that is effective in hooking in victims, but their modus operandi tends to remain the same. We can analyse and incorporate those typical behaviours in our systems—things such as bulk friend requests, poor feedback and other fake account characteristics. We can then use those to find those accounts and ban them.

When we consider these things, it is important to recognise that fraud, by design, is very hard to spot. It is supposed to be hard to spot for users, obviously, and, by its nature, it is hard to spot for our systems too, so we are constantly investing in evolving our systems to deal with it. It is also important to recognise that what we are dealing with is organised crime and organised criminals. They are sophisticated organisations that invest a lot of time and money in trying to get round the systems that we put in

place. That is why we invest so much money in trying to protect our users.

Lord Vaux of Harrowden: Thank you. Liz Kanter, do you want to go next?

Elizabeth Kanter: Yes, of course. Thank you very much for having us here today. Like everyone else on this call, we take this issue very seriously. We have observed, as Philip said, changing behaviours from our user community and, in particular, some of our advertisers. Although we do not see a huge prevalence of fraud and scams on TikTok, there are some actions that we have seen, particularly in the advertising space, and I want to call out a few examples.

One thing we have observed is that advertisers tend to comply with our creative policy or industry entry policies on whatever the category of content is, but what they do underneath is put a different landing page, so that when a user clicks through to the landing page there might be a QR code in the landing page that tries to take the user out of our app into another space that may contain fraudulent activity; or they have a landing page that is completely different from what the creative is. That is fraudulent activity that is not allowed on the platform. We banned over 10 million ads in 2021 containing that and other types of ad that violate our policies.

With regard to what we do to try to keep fraud off our platform, we take four different steps, in particular. The first thing, of course, is that in our product we try to create friction so that the product itself is not a place for fraudsters who try to create a hostile environment through fraud on TikTok. We do things such as our direct messaging platform. We do not allow users to contact other users on TikTok unless they are connected, so there is no unsolicited direct messaging. We do not allow users to send anything in direct messaging other than a TikTok video or text. They cannot send a link to a WhatsApp or send a QR code, or do anything that would take the user outside the TikTok environment into another space where there might be fraudulent activity.

We also have policies in place. Our community guidelines absolutely prevent frauds and scams on the platform and these policies are focused on preventing any type of illegal activity or fraudulent activity on the platform. We are very proud that we were the first company to take the FCA's list of authorised financial services companies. We did that in 2020 prior to any of our peers and we are proud that we did it voluntarily. Importantly, we take the equivalent of the FCA list in the UK in other European markets.

On processes, we have, like other platforms, a whole range of moderators who look at this kind of content, both on the organic side and on the ad side. On the ad side, we have a team called Monetization Integrity, which reviews ads to make sure that they comply with our industry entry policies and our creative policies. I can give you a sense of the numbers on the organic side in UK-specific numbers. In the fourth

quarter of 2021, we took down 85 million videos globally. We took down 2 million videos in the UK and, of those 2 million videos, 13,519 videos or organic content fell into the scam or fraud category. I share those numbers with you to illustrate the point that this kind of content is very low on TikTok, but we have very strong policies to keep it off the platform.

The other thing we do, and I will end on this, is the really important aspect of media literacy and education. We engage with a whole range of partnerships, including working with the ASA—the Advertising Standards Authority and organisations like UK Finance, who we partnered with on their Take Five programme. We had a financial literacy programme last year called #FactCheckYourFeed. We worked with people such as Tej Lalvani from "Dragons' Den" and Citizens Advice to make content on TikTok that was very, as we say, TikTok first, and our users engage with that. The dwell time, which means the time that people engage with the content and digest it, was four times higher than the average campaign of this type.

We think that that four-pronged approach is a very powerful way of keeping this type of content off the platform to prevent the fraud in the first place. Things like the educational initiatives that we do help us to protect our users from engaging in this kind of content.

Lord Vaux of Harrowden: Thank you very much. Graham Pullan, do you want to finish off?

Graham Pullan: I echo Philip's and Liz's sentiments. It is great to be here. Obviously, we take security very seriously. Fortunately, we have not had to reflect those changes over time, as we planned from the very beginning to put a two-step verification process in place for every person who joins our platform. This means that all our customers are verified at the very start of the process. We do it by matching the image of the user's face to their photo ID or their chosen photo ID, which in the UK is typically a passport or a driving licence. That is done using biometric face-matching technology.

The two-step process literally takes a few minutes to complete and is supported by a team of behind-the-scenes document checkers who make sure that no fraudsters can pass our checks. We also extract data from thousands of ID documents in over 200 countries or territories, which is done using optical character recognition. The data can be cross-matched between multiple providers, which provides us with very high levels of security. For obvious reasons, that process seriously discourages online scams and fraudsters. Should they commit any acts of fraud, they can be instantly identified.

From the outset, all our members are accountable for their actions. Should it be necessary, our moderation teams can easily monitor and trace any problematic scenarios back to the perpetrators. We can then respond quickly. This can simply mean taking somebody off the site for a short period, permanently removing someone from the platform or, in

very serious cases, escalating it to relevant authorities, such as the police.

As I have just highlighted, we already have several preventive steps in place, the first of which is ID verification. That process alone seriously discourages online scammers and fraudsters, as they cannot hide behind aliases or false profiles, because obviously we know who they are. By knowing who they are, we can report them directly to the relevant authorities. As for the future, we are working on ways to automatically exclude high-risk individuals such as those with relevant convictions or, for example, people listed on the sex offenders register.

The second preventive step is our AI moderation. This filters out inappropriate images at the handset, which stops them being uploaded from the handset to our platform. It also filters and blocks abusive language and hate mail through algorithms that can understand both the context and the semantics of what has been written. It flags up dubious images and texts for our human moderation team to view. Lastly, we build prevention into our design blueprints. For example, our members cannot view or interact with each other until they are fully verified; no content can be published or viewed until an account is verified. Real first names from a person's ID are always visible. We also verify members' ages; we can take their date of birth on the ID. This eliminates age-based scams, discourages grooming of vulnerable groups and allows our members to choose the age range that they wish to communicate with.

Lord Vaux of Harrowden: Thank you. No system is ever going to be 100%, so how effective do you think all of that is, Graham? Ninety-nine per cent, 80%?

Graham Pullan: Statistically, it is around 98% to 99%. As you say, no system is infallible, but it is pretty infallible. The fact that we have the behind-the-scenes checkers makes sure that it is virtually 100%. If anything goes through that we are not quite happy with, they are instant; they are on to it straightaway. They check it and nine times out of 10, probably 10 times out of 10 in actual fact, they spot fake ID, in this case, passports or driving licences.

Lord Vaux of Harrowden: Thank you very much.

Q136 **Lord Gilbert of Panteg:** Thank you for that. What you are telling us is that your real priority is the preventive work that you do. That is about proactive detection of content and removal. Philip, you said stuff gets through; you cannot catch everything. Whether 1% or 2% of stuff gets through or more, depending on your platform, some of that will be reported by users. I want to understand what that means. For each of your platforms, how do users report content that they perceive to be fraudulent? When they report it, what happens?

Secondly, perhaps you can tell us whether you detect fraudulent content yourself or whether it is reported by users. What do you do to stop bad actors getting back on to the platform? You may have identified someone

who is potentially risky and removed them or, following a report of fraud from a user, you may have taken somebody down. What do you do to stop them getting back or refining their fraudulent model?

Philip Milton: As you said, our primary aim is to ensure that users do not have to interact with fraudulent content at all. That is why we have invested so heavily in this area. Where they do, we make it very easy to report content or ads. If you go on to Facebook or Instagram, at the top right-hand side of every piece of content, be it an ad or a piece of organic content, user-generated, there will be three dots. You can click on that; it will give you various options including whether you want to report it and the reason you want to report it. That report will be sent through to us as an organisation, and the content will be reviewed within 24 to 48 hours. Then, if we find it to be in breach of our policies, or if we find it to be fraudulent, we have technology that can fan out and find associated accounts and associated content. We can, therefore, delete not just the piece of content that you have reported to us, but anything else associated with those accounts that we think might be fraudulent, and indeed the accounts themselves.

To prevent bad actors from reappearing, we can log the IP addresses and the device IDs that those accounts have registered to them and are using. We can block any future accounts that they attempt to open. It falls back into the focusing on bad actors point that I made at the top. We focus on accounts and false accounts, and use that as a barometer to try to stop fraud where we can.

Lord Gilbert of Panteg: Would you explain in a bit more detail what happens when you receive a report from a user? You say that it is responded to within 24 to 48 hours. Do you have a triage system where something that is obviously a new or emerging fraud, something clearly problematic, gets dealt with very quickly? How does stuff get from your automated systems to a human being?

Philip Milton: That is a difficult question, because the answer is that it really depends on the specific piece of content that has been reported to us. Very rarely is it clear-cut. As I said, fraud by its very nature is designed to be deceptive, so it will look very genuine, even to our systems. Our systems are trained to recognise that, but they do not always recognise it. First, it goes through an automated system nine times out of 10. Depending on whether it is hard to tell or if we cannot quite make a decision, it might then go to human review after that.

Lord Vaux of Harrowden: Thanks.

Elizabeth Kanter: Please remind me if in my answer I have forgotten some of your questions. I think I noted them all down, but there were quite a lot.

In terms of where the user can report, both the organic side and the advertisement is the same. When you see the content, you hold your finger down and you come up with a report option; there is a whole range

of categories on which a user can report misinformation, scammer fraud, whatever it may be. That goes through, and depending on the type of content—to the point about the blend of AI and humans—it will typically go to a machine to review the content. We recognise with this type of activity that the human element is critical, because it is not always very obvious when there is fraudulent content. We would have subject matter experts reviewing that content and understanding whether it was indeed a violation of our community guidelines.

The issue of recidivism or repeat offenders on the platform is something that we think about with this type of content, and all content on TikTok. If we see a repeat offender, we can find that content and have key words or signals related to that repeat offender and block that offender; we can ban their device. We sometimes take a video or content and bank it, or use it to train our machines so that they can detect it going forward. We look at banning a user, potentially banning a device or blocking a device as well as using their content to train our machines to catch it in the future.

To give you a couple of pieces of data on your questions about reports, we also give reports on law enforcement, which is a really important element of this ecosystem. Since September last year, we only had eight reports from law enforcement for information about an individual user. In some cases, we provided information. About 1,300 ads were flagged to us last year. We took down only 8.5% of those ads.

I use that figure to illustrate that it is important that in our case the industry entry policies, particularly in advertising, are really conservative with a small C in the things that we do not allow on our platform. TikTok does not allow crypto ads, get-rich-quick schemes, pyramid schemes or peer-to-peer lending. We have quite a broad list of things we do not allow. The categories we do not allow chime with what the FCA has said are the most prominent categories of advertising that could lead to frauds and scams. We already take an approach that tries to protect our advertising ecosystem in the first place. As I say, for user reports on the advertising side, we reviewed about 1,300 financial services ads and took down less than 10% of them.

I hope that answered all the questions. If it has not, I am happy to come back.

Lord Gilbert of Panteg: That is good, thank you.

Graham Pullan: First, I will explain how our users can report fraudulent activity and what steps we take once it is reported. Our members can report an account or a message instantly within the app. They can also block the offensive account from viewing them or messaging them. Those actions automatically raise a ticket in our system, which is then picked up by our human moderators, who review it and take the necessary action.

Human moderation is a very important part of the process, as it can pick up nuances that AI cannot. Our moderators have the authority to

suspend accounts while they are under investigation and, in certain circumstances, request that those users are removed from the platform. All these processes are organic, as our platform has a no-advertising policy.

Regarding the second part of the question—if removed from our platform, how do we stop a bad actor from reappearing under a new alias?—within our ID verification process we have a process called Remember Me, which does exactly that; it simply remembers past users' IDs. The process prevents bad actors from rejoining our platform; even under new aliases, they still cannot rejoin the platform. That said, we cannot be naive. Fraudsters try to find new ways around the barriers that are obviously designed to stop them. To combat this, our team continuously work on new measures to improve our abilities to identify previously banned users and prevent them ever rejoining our platform. For example, we are currently exploring ways of storing encrypted data and associations of data, such as the document numbers, with other personally identifiable information. This is to prevent a user returning with a second form of ID.

Lord Gilbert of Panteg: Thank you.

The Chair: Thank you very much. Liz, this may just be my ignorance about TikTok, but you mentioned that TikTok has no crypto ads. How would you stop a perfectly legitimate TikTok user, an influencer, trying to push crypto; it is not an advert but a user who has decided to recommend it, for example?

Elizabeth Kanter: It would depend on whether it was branded content and they had been paid by a crypto company; that would not be allowed. On the organic side, a user can talk about crypto. We prevent content that tries to inflate or promote a get-rich-quick scheme or an inflated lifestyle, but it is a very nuanced area, as you pointed to. On the ad side, we have very strict controls. On the branded content side, it is also banned. On organic, we have cautions around what kind of lifestyles are promoted around crypto. I could write to you a bit more on the nuances of our approach, if you would appreciate that.

The Chair: Thank you. That would be great.

Q137 **Lord Browne of Ladyton:** This is the first of a number of questions designed to test the effectiveness of potential methods of disruption. To some degree, we have entered this space anyway. This question is about the role of consumer awareness. How effective do you think consumer education campaigns are? For example, do you think users of dating apps know about tools such as reverse image search? Where does the balance lie between consumer awareness and victim blaming? Given your business model, Graham, maybe you could start, please.

Graham Pullan: Absolutely. Improving the general level of understanding for our users around cyber risk is of paramount importance to us. We have aligned our thinking with the national cyber

security strategy, in particular pillars 1 and 2, which strengthen the UK's cyber ecosystem and build a resilient and prosperous digital UK.

It is fair to say that customers understand the educational campaigns that are going around, but we feel that we need to make more people aware of the perils of online fraudulent activity, although the media in general seem to be helping these campaigns as the subject of online fraud or scams seems to be almost a daily topic in the newspapers or on TV. This has been helped by more recent documentaries such as "The Tinder Swindler", which was one of the most watched documentaries in 2022 and watched in over 90 countries.

Online daters are aware of tools such as reverse image search. To combat this on our app, pictures cannot be directly downloaded from the app. However, there are additional educational needs relating to the threat as it is a constantly changing environment. For instance, criminals now manipulate images before they use them in the hope that they will be undetected when using reverse image search. Within our duty of care, we endeavour to educate our users to the best of our abilities. Our AI moderation supports this by flagging potentially abusive content to the original poster, the receiver and our moderators.

As for where the balance lies between consumer awareness and victim blaming, we feel that there is a responsibility for adults to conduct themselves in a socially acceptable manner. Our belief is that if it is unacceptable in real life, it is unacceptable on our platform. Through various focus groups of varying demographics, I would say there is still a lot to be done to educate people. There is certainly awareness, but there is general apathy. People know that things need to change, and that is a given, but they do not have a clear view on what that looks like or how they could help themselves by becoming more aware.

We believe there is a need continually to educate customers in relation to online fraud and scams. Importantly, we believe there is a need significantly to improve cybersecurity in the UK. As for victim blaming, people are fallible by nature. Therefore, we believe that no one should be blamed for being scammed or being a victim of fraud. It has been shown that even the most astute people have fallen foul of online fraud.

Lord Browne of Ladyton: Thank you, Graham. Liz, the scale of fraud in this country is massive. It depends on who we ask, but we are told that somewhere between 39% and 42% of crime in the country is fraud-based. If we are to rely on consumer awareness of that, there is a massive task; it needs to be scaled up to a large scale, to a scale that engages with the size of the problem. Whose responsibility is that, or is it a shared responsibility? To what degree do you engage with it?

Elizabeth Kanter: Good question. You will not be surprised to hear that, of course, we share the view of this committee, law enforcement and the whole ecosystem that it is a massive problem, but we believe it is a shared problem. It is interesting. When you think about a tech platform like ours, it is very difficult to draw a straight line from a video on TikTok

to someone being encouraged to take money out of their bank account and hand it to a fraudster. I use that as a very extreme example to show that it really is a whole value chain responsibility, but we take our responsibility very, very seriously.

That is why I spoke before about the policies we have in place that are quite strict about which content is allowed on our advertising ecosystem. In our policies and our education, we are doing what we can to keep it off our platform, to make TikTok a hostile environment for fraudsters. We share your view, or the view that you mentioned, about it being a shared responsibility.

Lord Browne of Ladyton: Thank you. Philip, the whole ethos of social media is that you help create relationships and communities. Who takes the responsibility for who gets into those communities?

Philip Milton: That is a great question. It is important to say up top that it is incredibly difficult to spot a scam; that is the entire point of it. It is really important to teach people how to recognise the signals that come with those scams where we can. That is not me abdicating responsibility for that; we as a platform must absolutely do what we can to minimise users' exposure to those things. As I have said already, just as it is unlikely that we will ever completely eliminate fraud in society, so it is unlikely that we will be able to eliminate it completely online. We must arm users with information. It is not only information that will help us fight fraud, but it is a big piece of the armoury.

We have invested in several user education campaigns over the last year or so. On Facebook and Instagram just last month, we launched a nationwide campaign, with videos that ran across both platforms on things like money mules, investment scams, friend in need scams and a bunch of others; they are all available on our website if you want to take a look at them. We also had a campaign on WhatsApp with National Trading Standards that talked about message scams. We supported UK Finance's Take Five ad campaign, collectively with a bunch of other tech companies. We donated $1 million-worth of advertising to that campaign. That is all designed to bolster users' knowledge of the kinds of things that they might come across if they get past our various systems. As I said, we think that is a vital piece of the armoury against fraud.

Lord Browne of Ladyton: This is a relatively short question, but it is quite important. You all say that this is a number one priority. It may share the number one spot with some other things. In your respective terms and conditions, do you spell out to people who come on to your platforms that fraudulent behaviour will get you disqualified from them for ever?

Philip Milton: From a Meta perspective, yes, we do.

Lord Browne of Ladyton: Do you use the word "fraud"?

Philip Milton: Yes, we do.

Lord Browne of Ladyton: Liz, do you use the word "fraud"?

Elizabeth Kanter: I want to double-check our terms of service, but we do not allow our users to be taken advantage of. I would love to go away and look at that just to make sure I get it right and come back to you.

Lord Browne of Ladyton: It is a bit unfair, but I spent three hours today reading a set of terms and conditions. I have to admit that I did not completely read them all, because even in three hours, although I am trained as a lawyer, I could not get through them all. I did not find the word "fraud" anywhere.

Elizabeth Kanter: Our terms of service rely on respect for the individual user. We also have in our terms of service the right to take pre-emptive action against a user we think will cause harm on our platform. If we think someone like Tommy Robinson or the rapper Wiley is going to take action on our platform that may be harmful to our user community, we can take pre-emptive action and ban them from ever opening a TikTok account.

Lord Browne of Ladyton: Thanks. Graham, do you have the word "fraud" in your terms and conditions?

Graham Pullan: I honestly do not know if the word is in our terms and conditions, but fraud is not something we accept. If people try to commit fraudulent activity, they will be removed immediately from our platform and, as we said, they cannot get back on. There is no chance they will ever come back.

Lord Browne of Ladyton: Thank you. It is a personal prejudice, but I would be more persuaded of it being a priority if it was there.

Graham Pullan: No, you are absolutely right. It is a word that should be there.

Lord Browne of Ladyton: Thank you.

The Chair: You are all very welcome to check. Philip was pretty adamant, but if the others want to check and write to us on that, it would be terrific.

Q138 **Lord Young of Cookham:** The discussion so far has been about prevention and education. Can we move on to the next stage, where, despite everything that we have been talking about, fraud happens and money changes hands? We have heard in earlier evidence about mule herders, and we have been told that there are 50,000 money mules out there through whom the money passes. What steps do you take to prevent people being recruited as money mules? If they are recruited, what steps do you take once the money begins to change hands through the money mules to stop the transactions before any more take place?

Elizabeth Kanter: Yes, thank you. It is important to say that money muling, as you know, is organised crime. They are aggressive actors who

try to socially engineer our users to break the law, which is something we do not tolerate on our platform. We deal with that kind of content by working in partnership with law enforcement. It is the kind of content we might be asked for information about from law enforcement. If they detect that kind of content on our platform, we would, of course, share information with them if we had a valid legal request.

Our starting point on money muling is that it is not allowed on the platform. We have key words in place that are detected through our automated systems. We have human reviewers who can detect that kind of content. Like any content, it falls into the category of illegal activities and regulated goods and is something that we take seriously. In our community guidelines enforcement report, we have a strong record of proactively removing about 96% of that kind of content before it appears on the platform. We take a very serious approach to it. Like any of this kind of content, it is a partnership between us, law enforcement and other actors in the space. We will absolutely do our part to get that kind of egregious content off the platform.

Lord Young of Cookham: Philip, you mentioned money mules a few moments ago.

Philip Milton: Indeed, yes. Money muling is a trend that we have seen across a lot of different sectors over the last year or so, and we have been working with police and financial institutions to try to improve our response to it. In what we proactively do on our platforms, there are certain behaviours and trends associated with money muling that we can look for. We proactively scan content to look for those signals. We use things like key word detection. You often see in money muling people soliciting bank information, so we look for things like that across our platforms. Where we find it, we lock those accounts and people have to prove their authenticity before the accounts will be unlocked.

We can then, as I said in answer to an earlier question, fan out and find other accounts that are associated with that account—other pieces of content—and remove those too. I point to education in this piece as well, because often you find that money mules do not actually know that that is what they are. It is often a crime that people commit unknowingly. The mule herders know exactly what they are doing, but often it is a get-rich-quick scheme for people who might not necessarily know the implications of what they are doing. It is effectively money laundering. One of the videos I mentioned earlier, the nationwide campaign we did across Facebook and Instagram, was focused on money muling particularly, in part to help educate victims and people who might be lured into being money mules about the dangers of doing exactly that.

Lord Young of Cookham: Graham, this is perhaps less of an issue for you.

Graham Pullan: It is. Our platform has not experienced the recruitment of money mules yet. For us, it is all about preventing it occurring on our platform. As part of the prevention, we plan to implement text filtering

technology that will be used to pick up key words or phrases that highlight potential misconduct such as recruiting money mules. By doing that, we plan to filter the content before it reaches our target audiences. In essence, it stops them at source, although let us not forget that in our case the perpetrator is known to us, because we have their ID, which is very much part of the prevention process.

Prevention is ongoing, as we regularly review the identity of key words and language being used in our suspected scam activities. By following that process, we regularly feed new content into our new moderation algorithms. That allows our human moderators to monitor activity on key words and phrases in the hope that we can prevent the scams at source by automatically filtering messages containing known phrases associated with the recruitment, in this case, of money mules.

Another key opponent in the category of prevention is advertising, more specifically targeting advertising. Many social media platforms generate their income solely through advertising, and the product they sell to advertisers is users' data. Those advertisers can use the data to target specific groups, and, in this case, they could easily use it to target people to become money mules in the hope that they can create quick cash.

That is one reason why advertising is not permitted on our platform. Our users are our customers, not our product, and the safety of our customers is extremely important to us. Preventing scams such as recruiting money mules or the like is something we take very seriously, and any profile attempting to use the app for sale of goods or services will, as I said earlier, be permanently expelled.

Lord Young of Cookham: I have a final question for Liz. Are mules criminals or victims?

Elizabeth Kanter: Did you ask whether mules are criminals or victims?

Lord Young of Cookham: That was the question.

Elizabeth Kanter: It is a really interesting question. If people feel that they need to engage in the behaviour of money muling, they are probably a victim of the system gone wrong to educate them about the reasons why they should not be doing it and defrauding others. It is an interesting philosophical question. Those who engage in money mules are victims to some degree, but, ultimately, money mulers are criminals. We need to get them off the platform. We work with law enforcement to do that, and we take it very seriously.

Lord Young of Cookham: Thank you.

Q139 **The Chair:** I want to focus in this next question on Philip and ask about internet-based messaging services. Meta has three of the biggest in WhatsApp, Facebook Messenger and Instagram. We have written evidence from high street banks that 70% of the cases of investment fraud reported to them just between January and March this year started on Facebook or Instagram, either through advertisements, which we have

touched on, or through victims being directly messaged.

Cases of WhatsApp fraud, or fraud perpetrated through WhatsApp, particularly family fraud—parent and child fraud, I think it is called—have increased exponentially. WhatsApp is not just a messaging service; it has also become a calling service, because of voice over internet. Philip, I appreciate you have not been with Meta for very long, so if there are details that you want to follow up, that is understandable, but perhaps you could take us through what Meta does to prevent that fraud, particularly in relation to WhatsApp to start off with, both calls from overseas, which is where a lot of fraudulent calls seem to come from, and mass messaging and fraudsters using those messaging services.

Philip Milton: I am more than happy to. It is a really good question. The first thing is that WhatsApp is an end-to-end encrypted service. We think that that is an essential piece of technology in fighting fraud. It is exactly why all your bank transactions are encrypted. That kind of important personal information is encrypted, because it prevents fraudsters being able to see it. We think WhatsApp is a real leader in the market in offering that to users, but encryption is not where we stop.

In addition to encryption, WhatsApp is a number to number-based service. You need someone's number in order to contact somebody else. If you are contacted by a number that you do not know and that is not in your contact book, when the number first contacts you will immediately be asked to block or report that number, and you can move on if you do not want to do that.

We also use machine learning to scan for particular behaviours that are associated with scams. We look for things like bulk messaging. That is not generally normal behaviour, and that will throw up flags for us. We offer reporting tools for users as well and we encourage two-step verification. To focus on the education piece, I mentioned earlier that we did a campaign with National Trading Standards—"STOP. THINK. CALL."—which is entirely based on educating users about the dangers of message-based scams. It is important to say that it is an adversarial space and these things are hard to spot, but we think WhatsApp is in a good position to address many of those scams.

The Chair: On the WhatsApp calls, I understand that in October last year Ofcom asked phone networks to block internet calls coming from overseas that pretend to be from UK numbers. Are you able to tell if somebody appears to be calling from a UK number, but the call actually originated from overseas?

Philip Milton: I am afraid, Chair, that I do not know the answer to that question, but I would be more than happy to follow up to the committee.

The Chair: You talked about blocking if a number comes in. Perhaps you could take us through that a bit further. An awful lot of people—tens of thousands—appear to be falling victim to WhatsApp messages that look as if they are coming from somebody they know, often a family member, asking for money, because they are in an emergency situation. People

are falling for that, so if it was quite as easy as you say—we may go back to the consumer education point about people being more sceptical—surely you would be seeing it. Given the numbers, what are you doing to get ahead of it to prevent future victims?

Philip Milton: You are right; it is a mixture of proactive action on our part and user education on our part. Those are the two things we can do that will really help move the needle on that particular type of scam. As I said, if you receive a message from a number that you do not have in your address book and you do not know, you will immediately be asked to either report or block that number. It might be that you do not want to do that. It might be that you do not know the person yet, so, of course, you can ignore it, but that prompt will come up at the very top of the conversation if it is a number that you do not know.

Encryption is used across the platform for messages between people, but there are parts of the platform that are not encrypted. We can use machine learning on that to see where people are using images that may look like another image in your address book, but are not actually the same number for that image, if you see what I mean. If your mother is texting you, she might have a profile image that might be copied by someone who does not have the same number as your mother, and that will then be flagged up to users proactively to say that that person is not who they might seem to be and you might want to block or report them to us.

The Chair: Okay. I have a final question. I will come to Liz and Philip in a moment. Liz mentioned no direct messaging from people who are not contacts. Is that something you considered for Facebook Messenger and Instagram, where I think people can direct message you even if they are not contacts or people you follow?

Philip Milton: I believe there is a setting in Instagram whereby you can turn off the ability for people who are not your contacts to direct message you, but I would have to double-check on that and come back to you, Chair.

The Chair: Okay, thank you. Liz, you talked about direct messaging earlier, as I have just said. Is there anything else you want to add, particularly on the messaging service in TikTok?

Elizabeth Kanter: It is a closed environment in terms of the protections I mentioned before—the mutual follow rule and the inability to send links in messages. We have taken that view not only for this area, but for areas like grooming and the worst, most egregious types of crime. I would leave it there on that functionality. People do not really come to TikTok for direct messaging. They look at us as an entertainment platform. Even though that is true, we still take protections and put safeguards in place on direct messaging. I will leave it there.

The Chair: Graham, is there anything you want to add on the messaging side of things?

Graham Pullan: I have a slightly different view from Philip, so maybe I can give you that view. Apps like WhatsApp, Facebook Messenger and similar internet-based messaging services are end-to-end encrypted, as Philip said earlier, which means that not even the company hosting or facilitating the service can see what the users are doing. That is promoted as a safe and secure way to communicate, and, as Philip said, it is a very safe way of communicating.

However, end-to-end encryption has a serious downside. It provides its users with a platform in which they can be totally anonymous, allowing them to hide behind fake profiles and aliases. That scenario provides ill-intentioned individuals and groups with an ideal set-up, which gives them secure end-to-end encryption so that nobody can see what they are doing, in a place where they can be totally anonymous and have the freedom to commit criminal, illicit or fraudulent activity in what can only be described as a black hole.

The only way to assess whether communications made via this route are legitimate is to remove anonymity by making it impossible for users to create fake profiles and aliases by ensuring that all users go through an ID verification process before they join those internet-based services. It also offers a balanced scenario. On one side, we need to protect users' privacy via encryption, but, on the other side, we need to protect users from criminal, illicit and fraudulent activities by removing the ability for anyone to create aliases or fake profiles.

The Chair: That is very helpful. Thank you very much indeed for that.

Q140 **Lord Browne of Ladyton:** I want to come to data sharing. I have a growing interest in reading the terms and conditions of social media platforms and other online businesses. It seems to me that a significant amount of your terms and conditions is devoted to data, how you can handle the data and what you can do with the data that belongs to the people who contract with you. It is a fairly simple contractual process; you tick the box or you do not deal. There is no negotiation about it. Against that background, responders to our call for evidence have credibly said to us that sharing data within sectors like yours, across sectors and with banking, police and other people is an important aspect of trying to interdict this sort of behaviour or to investigate it.

I would like each of you to try to answer this question. Do you share data about fraud risk and identifiers within your sector, across sectors and with law enforcement? If you do not, what are the barriers to it? Does GDPR in particular help or hinder the process? Are you willing to do it? If so, what change would encourage you to do it? Whoever wants to start can volunteer.

Graham Pullan: I do not mind starting. We do not have first-hand experience of sharing data on fraud risks within our sector, across other sectors or with law enforcement at the moment. However, we have an internal policy on how that type of data is shared with the police or other law enforcement authorities. The policy is regularly reviewed to ensure

that it is aligned with the ICO guidelines and Parts 2 and 3 of the Data Protection Act. Our understanding is that GDPR can hinder the process, as it inhibits sharing the details of suspected scammers or predators with other platforms, which in turn could prevent repeat or new attacks across other platforms.

Where evidence is available regarding specific levels of activity, it would be very useful to have a method that identifies and shares details of high-risk individuals or personas, perhaps in the same way that financial institutions share data on potentially fraudulent activity. Such a scheme would be extremely important to law enforcement and policymakers, as it would help them to understand trends and behavioural habits by creating a large, shared dataset.

Lord Browne of Ladyton: Graham, can we go back to your understanding? You believe that GDPR hinders. Has that view been formed by legal advice that you have been given, or is it just the impression in your industry that it does?

Graham Pullan: It is an impression. I have not had legal counsel on that. An impression we get is that GDPR can hinder the process, because it stops you sharing details.

Lord Browne of Ladyton: I have to say that we have received evidence that the opposite is the case, but we will not go into that. Liz, maybe you could address this question. Does your business share data voluntarily? Do you think the sharing of data is restricted, and in particular does GDPR form a barrier?

Elizabeth Kanter: You will not be surprised to hear that we are in favour of information sharing around new techniques for defrauding users or on emerging trends, case studies and best practices. We do that across a range of industries and in this one.

We are members of the Online Fraud Steering Group, and we have been such since the beginning when it was created and came into force last year. The Online Fraud Steering Group is a place for sharing intelligence and information about trends that we see in banks, law enforcement, government and industry. I will respond to your question in terms of our relationship with law enforcement. We have a relationship with law enforcement where they can ask us for information about an individual user. We report twice a year on the number of law enforcement requests we get.

In the UK, we get requests from law enforcement on a variety of areas, including scams and fraud, and it is all governed by the Investigatory Powers Act. An IPA request is a very narrow request for information about an individual user. When we get a request from law enforcement, our legal team looks at it in relation to GDPR. In those cases, the request is so narrow that we provide only the information we are asked for, even if we spot information about the particular user that might be helpful to law enforcement. We do that because of GDPR.

If we shared information about one of our users and jeopardised their privacy or their data protection rights, we could face a very large fine because of GDPR. I spoke with legal colleagues about this just as an anecdote, and they said that they find that the current data protection regime is hindering our ability to proactively share information with law enforcement.

We could change that or address it, to allow us to have more freedom in what we share, through the data reform Bill that will be introduced, we believe, in the next Parliament. It could look at something that we refer to as a good Samaritan principle, where we could share information that we think will be useful to law enforcement, but under a good Samaritan principle we will be protected when we share that information and have the safeguard of knowing that we will not face a potential fine under GDPR. Yes, we think GDPR is restrictive in what we can share, but we think there is an opportunity in the data reform Bill to address that and, hopefully, allow us to share more information more proactively.

Lord Browne of Ladyton: Thank you. Do you think your lawyers would share with us a couple of paragraphs on why that is the case with GDPR?

Elizabeth Kanter: I will not commit, but I will ask them. I am sure they would be delighted to help on that.

Lord Browne of Ladyton: When I was a Member of Parliament, in the main town of my constituency, when a gang of shoplifters came to town and were discovered in one shop, the shop would immediately phone round all the rest of the shops to say, "They are about in our environment, and these are the people". If they had photographs, they shared them. I do not remember any of them getting into any trouble for it. Philip, what about sharing data about people in your community who may well end up in somebody else's community shortly?

Philip Milton: It is a great question that really gets to the nub of the issue. The truth is that none of us individually will be able to solve the problem. To do that, we need to work collaboratively with each other in the industry, with government, with regulators and with law enforcement. I have said a couple of times that safety and security is our number one priority. GDPR is an important part of that, but it definitely creates some conflicts and some reticence to share data, as Liz outlined. We are committed to working with others to create a system for sharing data in a meaningful but privacy-safe way.

We are also members of the Online Fraud Steering Group that Liz mentioned. That includes law enforcement, industry, government and regulators. We are a member of Stop Scams UK. Both those groups are very focused on exactly the question of how you take learnings from a tech company and share them with a telecoms company, banks, government, regulators and law enforcement, and do it in a way that is compliant with the law. We are absolutely engaged in that process.

Lord Browne of Ladyton: Thank you very much. That is potentially

very helpful. If any of you have any evidence of anyone falling foul of GDPR for doing that and being fined heavily, could you bring it to our attention? I cannot find any evidence of that anywhere. I may not be looking in the right places, but I cannot find it.

The Chair: Thank you. That sounds like a question for the lawyers. I think Liz is probably wise not to commit on their behalf, but we appreciate you asking them, and we can also ask the ICO. Thank you.

Q141 **Baroness Henig:** In a way, my question follows on from the discussion that has just taken place. At various points in questions earlier there were references to working with law enforcement, the police and so on. Now we get to the nub of things, and we find that there are actually big problems with data sharing and that working with law enforcement and with various agencies may not be as easy as you implied earlier. Can I look at this in a bit more detail? First, when working with the police, do they come to you or do you go to them? What normally happens? How significant are data-sharing issues in the relationship?

Philip Milton: As I said before, the question is really pertinent. Our primary focus is to try to prevent this from happening at all. I cannot stress that enough. We know that we need to collaborate with law enforcement and with others to do what we can to maximise our efforts.

We have a dedicated global law enforcement outreach team, with a lead based in London. They respond to requests from law enforcement. They also deliver training for law enforcement. We train partners in law enforcement on how to use our systems, how to make a request for information, what our policies are, what they mean and what they can do around those. We work closely with the City of London Police and its dedicated card and payment crime unit. It is the national lead on fraud. It is able to report to us through a reporting channel.

We work with the OFSG. It includes law enforcement in the collaborative solutions that I mentioned. Ultimately, the biggest deterrent to these criminals will be to increase the likelihood that they will be caught for the crimes that they are committing on our platforms. That is why we think these kinds of things are so important. We will not be able to do that without a proper process of data sharing, which is why we are so invested in those groups.

Baroness Henig: What would you like to happen?

Philip Milton: I think we are doing what needs to happen. By joining those groups, by bringing together not just tech companies but telecommunications companies, banks, law enforcement, regulators and government, we are able to start talking about where the barriers are and what we can do. We are just at the beginning of that process, but the fact is that we are all incredibly engaged in it. I have been to several of the meetings. They are held very much in a spirit of openness and a genuine attempt from all around the table to try to work together to see what we can do. There will be barriers in the way with the laws that are

in place, and we will come across those as we go through the process, but we are absolutely committed to doing what we can to share data better.

Baroness Henig: Liz, you talked earlier about the problems with sharing data with law enforcement and said you wanted to see some legislation to deal with those. Is there anything else you can tell us about how the relationship could be made more significant, so that information can be shared more freely?

Elizabeth Kanter: I will not rehash what Philip said about Meta. We have a similar infrastructure in place, with our global head of law enforcement sitting in Dublin, and colleagues across the UK working with the NCA, the FCA and the Financial Investigation Unit. You asked whether law enforcement comes to us or we go to them. In this case, law enforcement would come to us and ask us through the IPA, the Investigatory Powers Act, for information on our users. We provide very limited information on our users.

As I mentioned before, in seeing content, whether it is organic content or in the advertising space, that we think could be helpful to law enforcement, there is no infrastructure in place at the moment, or a framework or code of conduct, for sharing that information that safeguards the user, safeguards us as a business and helps law enforcement. If we could square that circle and find a mechanism for information sharing that protects all the different actors in the ecosystem, we would be very glad to engage in that conversation.

The Online Fraud Steering Group is having the conversation and it is proving very tricky. It is very tricky to satisfy everyone. Different players in the ecosystem want different information. It would not be appropriate for TikTok to provide the banks with information. That is not our role.

The other thing that we are concerned about is that, if you provide information about a user before you know whether they have indeed engaged in a criminal offence, are they guilty by the sharing of the information? We do not want to prejudice decisions. There are a lot of different moving parts in this space. We are having conversations in the Online Fraud Steering Group; they have been going on for quite a long time. We will continue to engage and do what we can. We work with law enforcement. We work with the FCA, the NCA and the City of London. We will do what we can to share information within the confines of the law, and, as it evolves, we will work to that as well.

Baroness Henig: Thank you. Graham, do you have any thoughts in this area?

Graham Pullan: Being a new company, we have not needed to work with the police or wider law enforcement yet, but when we do, the processes I mentioned earlier will allow us to review and refine them. One of the things that makes us slightly different is ID verification—the fact that everybody on our platform is ID verified, so there is no

anonymity. That makes a huge difference, especially for the police and wider law enforcement, because you know who these people are. I take Liz's point that you have to be very careful with that data, and you do not want to set someone up in a situation, but should that be the case, we know who our members are.

Baroness Henig: Thank you.

Q142 **Viscount Colville of Culross:** Good afternoon. I would like to start by putting a question to Philip Milton. You said in your first answer that Meta has put £13 billion into combating fraud. However, we have received written evidence from the TSB that says that 70% of cases of investment fraud in the first three months of this year started on Facebook or Instagram. The Online Safety Bill is making its way through Parliament. Do you think that big platforms like yours should be responsible not only for stopping fraudulent adverts, as is in the Bill, but for stopping all fraudulent content on your platforms? Would that encourage you further to combat fraud, or would it have a negative consequence?

Philip Milton: Thanks very much for the question. I would like to correct one point before I try to answer it. It is 13 billion dollars, not pounds. Apologies if I said pounds.

On your question, we very much welcome the Online Safety Bill. We have been calling for regulation in the online space for some time, because the decisions we take as a platform, especially as a very large platform, involve balancing competing interests all the time, and we do not believe that we, as a private company, should be solely responsible for doing that. We very much welcome the OSB and the principles that it sets out.

We have some concerns about fraudulent advertising being included in it, primarily because there is a pre-existing process going on called the online advertising programme, which we may go on to. That is a proper consultative process, and it considers the same issue. That is our primary concern. We think it should go through that proper consultative process.

It is important to say that we have not waited for legislation to protect our users. Some of the things I outlined in answer to the first question are what we do to prevent users being exposed to fraud. We do that without the need for legislation, because we believe it is our responsibility as a platform.

Viscount Colville of Culross: There obviously will be political pressure to try to extend that clause so that it covers all fraudulent content on your platform. What effect would that have on your company?

Philip Milton: I believe that, as it is currently drafted, it covers organic content, and the new edition covers advertising and paid-for content. As it is currently set out, it would, in fact, cover everything.

Viscount Colville of Culross: You mentioned the online advertising programme that is being looked at by the Government and will report, hopefully, later this year. Should it incorporate all the media agencies,

the intermediaries and the publishers? Why is that so important?

Philip Milton: We very much welcome the online advertising programme. It is aimed at increasing accountability and transparency, which we think is absolutely right. That cannot be a bad thing for online advertising. We think it should include the entire system. That is why we are so supportive of the consultation; it takes a proper holistic view of the entire piece. We think the existing system is really effective in dealing with many of the harms that DCMS has set out.

You may have heard from other people giving evidence that the ASA is just about to launch a thing called the intermediary and platform principles, which we think is a big step in the direction that the online advertising programme seems to be going, demonstrating, we think, the flexibility of the existing self-regulatory system to flex and adapt to what is a very fast-moving market. We are keen to engage and understand what else the Government think we might be able to do to mitigate any of the harms they have identified in the consultation.

Viscount Colville of Culross: Thanks very much. Graham, what are your concerns about the fraud clauses in the Online Safety Bill?

Graham Pullan: Most of our activities and processes are already aligned with what is being requested in the Online Safety Bill. However, the Bill and anticipated regulations from Ofcom have prompted the team to review our current policies and make any necessary amendments moving forward. The team considers it to be a continuous improvement process, and we do not foresee negative consequences from the Online Safety Bill, as we believe it is very necessary.

We would like to see the online advertising programme tackle the evident lack of transparency and accountability across the whole of paid-for online media. Our hope is that the online advertising programme, which is looking specifically at paid-for online advertising, will, as it states in its consultation paper, unpick the intricacies of this market by looking closely at the roles of each of the actors in the ecosystem and how they facilitate the minimisation of harm, which, in our opinion, should also include the gathering and selling of people's personal data, which in turn will create a sustainable system that people can finally trust.

Viscount Colville of Culross: Should the findings of the advertising programme be voluntary, or will legislation be needed to make sure that the harm that has already been specified by the CMA, for instance, will be dealt with effectively?

Graham Pullan: I think it should be dealt with effectively. Online advertising is harmful, especially in the way that a lot of social media platforms use their users' data and sell their users' data, which, as we all know, is the way they make money. Philip's company made $86 billion in 2020 on advertising revenue worldwide. It is big business.

Viscount Colville of Culross: Liz, do you, like the others, welcome the

fraud clauses in the Online Safety Bill?

Elizabeth Kanter: Yes, of course we do. As Philip said, we do much of what is being called for in the Bill already. I mentioned the FCA list. We have policies that prevent frauds and scams in the organic and the advertising side of TikTok. We welcome it to try to make a level playing field so that other players will level up in what they are doing in this space. We are doing much of what it calls for already.

Viscount Colville of Culross:, but it will not be a level playing field, because it is only going to be for category 1.

Elizabeth Kanter: That is a fair point. Yes, for category 1 companies.

Viscount Colville of Culross: Will it have a negative effect? One of the things that people have been saying is that, if we extend the fraud clauses to the smaller categories 2A and 2B, it will stifle innovation and competition. However, surely it will also be rather good for combating fraud.

Elizabeth Kanter: We shall see what comes out of it. I hope that would not happen. We are currently down as a category 1 company. We are focused on what we can do to create a frictionless place and uphold our responsibilities to prevent fraud on our platform. That is what I am mostly focused on.

Viscount Colville of Culross: TikTok is in partnership with the ASA to bring accountability and transparency to advertising regulation. What are you hoping for from the online advertising programme? Do you think it can clean out the harms that we have seen and the extraordinary complexities and monopolies of the digital advertising market?

Elizabeth Kanter: I share your view 100% that the digital advertising market regulatory environment is very complex, with lots of different players—the ASA, the FCA, the CMA, the ICO—all having a part to play. Our hope for the online ads programme review is that regulatory coherence is brought into the advertising ecosystem, looking at the Digital Regulatory Cooperation Forum as a model for bringing regulators together to talk about issues, potentially bringing the ASA into the DRCF so that it can have a voice and provide regulatory coherence. At the moment, there are a lot of different competing systems in place for us in the advertising space, and having that simpler system would make it a lot easier to comply with, for us in particular.

Viscount Colville of Culross: Thank you very much.

Lord Allan of Hallam: I want to talk about digital identity, but before we do that, I want to clarify a couple of points on advertising policy. We had Google here last week, which told us that restricting financial services ads in the UK only to bodies registered with the Financial Conduct Authority was a major step forward. I think I read something about Meta doing that, Philip. Can you clarify whether you are committed to restricting ads on Facebook and Instagram only to FCA-registered entities?

Philip Milton: Yes, we are. That process is ongoing. We are on-boarding the FCA as we speak, and that will be rolled out by the end of this year.

Lord Allan of Hallam: You do not have a firmer date than some time in 2022.

Philip Milton: It is H2 this year.

Lord Allan of Hallam: Okay, that is great. Liz, you explained that TikTok started doing FCA restrictions a while ago. I thought you went further. It would be helpful if you could clarify. What kind of financial services are allowed to be advertised to people in the UK on TikTok?

Elizabeth Kanter: Yes, we took the list in September 2020, quite a while before anyone else did it. I need to go away to give you a specific list of the categories that are allowed on the platform, because I have been more focused on what we do not allow than what we do. Perhaps I could write to you with categories that are allowed. It would be any regular financial services that are authorised by the FCA. I would be happy to give you a category list.

Lord Allan of Hallam: It would be helpful just to understand what is legit.

Elizabeth Kanter: If it is authorised by the FCA, it is legit. Let me see if I can give you a clearer categorisation.

Q143 **Lord Allan of Hallam:** That is great. Excellent. Thank you very much. Coming on to digital identity, Graham, you explained to us earlier how you were offering a gold-standard verification service out of the Sheffield Digital Campus, which is very exciting. I am curious. I understand that you use Yoti as your provider of identity verification. Can you tell us how much that costs and who pays the costs? Is it you or is it your user?

Graham Pullan: Our users pay the cost once they go through the ID verification. The process at the beginning is free. They can go on to the site and start to look at the site, but once they go through the ID verification it is part of the subscription cost.

Lord Allan of Hallam: How much is that, more or less?

Graham Pullan: If you go for a monthly subscription, it is £9.99, but if you go for three months or six months it is less. It is less than a lot of our competitors in the marketplace.

Lord Allan of Hallam: About £10 a month, and that includes the identity verification.

Graham Pullan: The ID verification is a one-off scenario, because once you have done it you do not need to keep doing it. You have the same ID and you will never change your ID, so it is a one-off cost.

Lord Allan of Hallam: That is very helpful. What is your view of the Government's digital identity framework, which seems to be encouraging

more users of these kinds of systems and interoperability between them?

Graham Pullan: It is what we have been campaigning for, as we very much believe that mandatory ID verification is the future, to ensure the accountability of individual content producers in whatever form. There are three points that we particularly like in the Government's digital identity framework. The first is the need for a principles-based approach spanning privacy, transparency, inclusivity, interoperability, proportionality and good governance. Fluttr was founded on those core principles, which in turn have enabled us to use ID verification from the outset. It is good to see, from our point of view, that the Government are endorsing this kind of approach and that their principles will be reviewed annually so that they can keep in line with any legal or other development in the UK.

Secondly, we welcome the fact that the Government have signalled that there is legislation in the works to ensure that digital ID can be used as broadly as possible. Finally, there is the fact that the Government intend to open up traditional data sources, as there are specific datasets that the Government control that could be used to combat fraud, such as DVLA data, death registers and the like. The document checking service pilot is under way, but it is currently limited to passport data. In our opinion, if the Government want to show that they are serious about using digital identity to stop fraudsters, they need to think about enabling other key data to be checked with digital identity providers. That would make it easier for companies like ours to identify fraudsters and conduct our own investigations into nefarious activities by our members in order to make sure that the appropriate preventive action is taken.

It is a resounding yes from us. We believe there should be mandatory ID verification for all users of online platforms, and that digital ID should be used as broadly as possible to tackle fraudulent activity.

Lord Allan of Hallam: Thanks very much. I will come to the other two platforms. What do you think about mandatory ID verification, first, for advertisers and, secondly, for all users?

Elizabeth Kanter: On advertising, we have a system whereby if an advertiser wants to work with our creators and create branded content, when it comes on to the platform it needs to submit its company name, the company name needs to match its website, and it needs to match what is on its business licence. As a second step, we require that it uploads on to our platform government ID to verify that it is a business. Then we have manual reviews to double-check that it is a legitimate business. That is on the advertising side.

If the Government introduced a digital identity framework and a rule was set in place, we would, of course, comply. We would be happy to engage with the Government in conversations. We are watching that and we will see what happens, but at this point our position is that if it comes into force we would, of course, adopt it.

Lord Allan of Hallam: Is your preference for ordinary users of TikTok to

have mandatory ID or not to have it?

Elizabeth Kanter: At the moment, we do not require any sort of identification from our users. I do not want to take up too much time, but we did a round of research with Internet Matters, talking to our users and to some of the user community from across Europe, and their view was that a mandatory system of requiring a passport or photo ID was not something that users wanted to engage with. Their preferred solution for age assurance was through the app stores, having Google and Apple play their part in verifying age and identity. That is what our research said. We listen to our users when it comes to this kind of issue.

Lord Allan of Hallam: Thank you. Philip, for the Meta properties, are you in favour of mandatory identity verification for advertisers and for users?

Philip Milton: In terms of advertisers, we take what we call a harms-based approach. We do not ask all advertisers to verify, but where there is potential risk to users we raise the bar for verification. We have already talked about us on-boarding the FCA. All companies wanting to place financial services ads will need approval from the FCA by the end of this year. We have a set of restricted ad categories across our platforms that require additional authorisation steps—things like alcohol, gambling, branded content and indeed politics.

One thing I would like to flag is that not all people in the UK have a form of identification. The Electoral Commission, I believe, did a piece of research on that which found that 3.5 million people in the UK have no form of ID. The DVLA found that just 53% of black people and 61% of Asian people over the age of 17 had a full driving licence. That is an awful lot of people to disfranchise from being able to advertise or being able to use a service as an organic user, and we think that a balance needs to be struck there.

We are engaged very much in the work the Government are doing on the digital identity framework. It is still very much in early development. We are supportive of the principles it sets out, but we flag in particular that there are costs of requiring photo identification. The cost is that you can risk disfranchising a large part of society.

Lord Allan of Hallam: Your preference is not to have mandatory ID for ordinary users.

Philip Milton: Yes, that is correct.

Lord Allan of Hallam: Thank you.

Q144 **Baroness Bowles of Berkhamsted:** How would you respond to the potential introduction of a "failure to prevent" duty to incentivise action by companies whose platforms are used by others to facilitate fraud? What would you do differently, or what would you do faster if there were such a requirement?

Philip Milton: As I said in answer to an earlier question, we have been calling for regulation in the online space for some time. We are really supportive of the OSB and of the aims that have been set out in the online advertising programme. It is hard to comment on a specific duty without seeing the detail behind it, but I will say that we believe platforms should protect their users. We have not waited for regulation in order to do that, and all the things I hope I have been able to lay out for you today illustrate that. We think it is important to avoid a kind of waterbed effect.

In answer to an earlier question, another person giving evidence talked about what happens when category 1 platforms that are already doing quite a lot on their platforms to prevent fraud are given additional duties to do that but everyone else is not given responsibility to do it. You might see a waterbed effect where the fraud flows from one area of the internet to another, and we think that would be a bit of a perverse outcome.

That is why we think the online advertising programme is a good place to talk about this: because it takes a more holistic view and is a more consultative process, and considers the entire cross-section of the online advertising industry. We think that is the right place for it.

Baroness Bowles of Berkhamsted: On failure to prevent, there are criminal offences already with regard to bribery and tax avoidance. The other side of that is that you have a reasonable defence if you have procedures in place. Do you feel confident that your procedures would withstand that kind of test at the moment?

Philip Milton: As I said, it is really hard to comment without seeing the specific duty and the detail. We are absolutely confident that the measures that we take are industry leading. That is not to say that we do not constantly seek to evolve them. Fraudsters continually evolve their habits and their processes, and we need to do that in order to catch them.

Baroness Bowles of Berkhamsted: I think I get the idea that you are trying to avoid saying that you do not want something, because basically it is not a failure to prevent something and that is it. The test is your defence, and you know what your defence is, because you are already doing it. If there were that kind of requirement, whether a duty or as strong as an offence, do you think it would help you if it also applied to other actors such as telecoms companies, given the role of spoof numbers and so forth in fraud?

Philip Milton: It is absolutely a shared problem. Fraud often does not just span sectors. One piece of fraud can span our platform, the telecoms platform, banking and real life. Therefore, the collaborative efforts of the Online Fraud Steering Group and Stop Scams UK are absolutely vital in being able to stop it. Yes, it needs to be a shared problem.

Elizabeth Kanter: My response is fairly similar. To keep it brief, we have to see the duty to better understand what it will look like in practice and

how it will sit next to the existing regulatory framework. It is difficult to comment on something we do not have.

As Philip said, we think it is a shared responsibility among all the players. Anything that can be done to eliminate fraud and remove it from the ecosystem is a step in the right direction, but it is difficult to comment on something where we just do not have enough detail to provide a robust view. I would be cautious on this, because I would like to see how it fits in, but I understand that it is being discussed, and if it goes forward we would be happy to engage in the conversation when we have more details about it.

Baroness Bowles of Berkhamsted: I guess the legal point, if somebody said that you had not done enough and they were able to take it to court, would be whether you thought that what you were doing already would provide you with a reasonable defence. That is basically looking at it from that side.

Elizabeth Kanter: I have tried to make it clear that we are doing quite a lot already through our voluntary commitments. The Online Safety Bill will put new commitments on us. We are unique as a platform in being regulated already by Ofcom and its video-sharing platform regime. We have quite a heavy regulatory burden in this space already, and we take that regulatory burden and responsibility very seriously. We have done so much already that I am not sure I can say much more than we take the responsibility seriously. I understand the question, but I would leave it at saying that it is a shared challenge, and we think that all players in the ecosystem need to take their part to try to prevent fraud happening in the first place.

Baroness Bowles of Berkhamsted: I take the point. You are saying that if there is something like this it should be widespread and not just the big players. Graham, do you have anything additional on that?

Graham Pullan: Just a short answer. We feel this type of duty is long overdue. Currently, we feel there is very little action being taken against companies that allow fraudulent activity to take place on their platforms. This is positive. Such action should be taken against companies that fail to prevent fraudulent activity.

Baroness Bowles of Berkhamsted: The point is that if you are not doing everything that you could be doing, something like this would catch it.

Graham Pullan: Absolutely, yes. I think it will stop a lot of companies making excuses, which they do, or trying to use other ways to get around it. There are fraudulent activities taking place on lots of platforms at the moment, and this kind of thing needs to be actioned against.

Baroness Bowles of Berkhamsted: Thank you.

Q145 **The Chair:** Thank you very much indeed. We have discussed lots of different issues. Is there one policy recommendation that you would

make to the Government in this space? You have all talked about wanting to prevent people being victims of fraud, but is there anything that would be a game-changer?

Graham Pullan: Mine is the same as it has been all the way through. Our recommendation would be to have mandatory ID verification. That process would make a big difference for all users on all online platforms. If they did that from the outset, a lot of the things that happen at the moment would change radically. That is something we feel passionately about and would recommend to the Government.

The Chair: Thank you. Liz, one recommendation?

Elizabeth Kanter: I will give two if that is okay. One is very simple. The FCA has its list that some of us have taken and some of us are going to take. We would love to see that list digitised. Fraudsters can look at that list and understand how they can impersonate companies, so the quicker we can ingest a list like that, the better.

The other thing is a broader point that I made before, which is the whole point about regulatory coherence and looking at how we can leverage the DRCF to potentially include the NCA, the National Economic Crime Centre or law enforcement to broaden its scope, which could be a good way of providing coherence in this complicated space. Those are the two recommendations I leave you with.

The Chair: Thank you very much. Philip, do you have one recommendation?

Philip Milton: I agree with what Liz said. Mine would build on her second point. Our recommendation would be for the committee to recommend that the Government have a Minister whose sole focus is fraud: a Minister for Fraud. As I said, fraud is a vast and sector-crossing problem, and because of that it crosses many Ministers' desks, but there is no one with overall responsibility or a cross-cutting view. I have said a couple of times that I think solutions to this problem require collaboration between government, industry, regulators and law enforcement. We think having a Minister for Fraud would really help those efforts.

The Chair: Thank you all very much indeed. As I said at the start, we are very grateful for your time and your input. There are a few areas that some of you are going to come back to us on with further detail. Please do that. For the purposes of this afternoon, I thank everybody for participating.