Written evidence submitted by Meta

Thank you again for inviting me to give evidence to the committee earlier this month on the important issue of fraud.

As I set out during the hearing, Meta takes fraud extremely seriously and invests heavily in tackling fraud. Doing so is a priority for the business because all our platforms are based on providing a positive and enjoyable experience for the people that use them. If we fail to do so people will use our platforms less and the same is true of advertisers. We are directly incentivised to ensure people who use our platforms are as safe as possible from fraudsters and scammers.

We use cutting edge technology in tandem with human experts to detect, prevent and remove fraudulent activity from all Meta platforms. By its very nature however, fraud is sophisticated, constantly evolving and cuts across industry and society both online and offline. We are therefore committed to working with others to find solutions, and we are proud of the work we are doing to achieve this, having spent $20 billion since 2016 on ensuring safety and security on our platforms, $5 billion of which was in the last year alone.

You asked me to follow up in writing on a few different points, both during and at the end of the evidence session. Please see below further information in answer to those specific questions.

The Government's fraud strategy

The Government's fraud strategy contains a lot of good ideas and represents an important step in bringing together a coherent strategy to tackle the issue of fraud. Meta is proud of the work we have done with the government and others in the tech sector as part of this strategy to deliver the online fraud charter in less than half the time it took to deliver other sector charters.

Outside of this work, Meta believes that there are four areas that will be key to driving down fraud in the UK:

1. **Increased and sustained investment in law enforcement's capability to prosecute the criminals behind these crimes.**

According to Home Office figures, Fraud represents 40% of all crime but just 1% of police resourcing. This means there is no real deterrent to take part in these crimes and until that changes fraud will remain at high levels. The new National Fraud Squad announced in the strategy is a small step in the right direction (whilst there are to be 400 new specialist officers recruited under the strategy, this should be compared to the fact that there are 233,832 FTE police workers in the UK). However, this investment needs to significantly increase and then be maintained over a number of years to be effective.

2. **Following the money**

The most effective way to drive down fraud is to follow the money. Banks are in control of this money. They are in control of the accounts involved, both the sending and receiving accounts. They know the identities of the holders of those accounts. They control the payment mechanisms through which the money is transferred. They are both the first (opening a fake bank account) and the last (laundering the money) link on the fraud chain and have the most visibility and insight into the crime that is taking place. Given this, there are a number of important steps that the government should require banks to take to reduce fraud.

- According to Anthony Browne MP (the previous Anti Fraud Champion) the introduction of a faster payments system in the UK with no fraud protections is a direct contributory factor to the rise in fraud in the UK. Banks should slow down payments to new accounts and stop unusually large payments, including those which accumulate over time so they can properly investigate whether the payment is legitimate or not.
- Banks should introduce a way to reverse payments when fraud is identified. Banks should work with international counterparts to repatriate funds when they are moved abroad. Repatriating funds to victims will vastly reduce the incentive for fraudsters.
- Banks should improve and standardise verification across the industry and should do more to prevent fraudsters from opening new accounts after they have been removed.
- Banks should do more to root out mule accounts and identify those banks who are most commonly the recipients of fraudulent transactions.

3. **Nation State collaboration**

City of London Police estimate that over 70% of fraud either originates abroad or has an international element. The UK government must drive cross border collaboration

between Nation States and use criminal proceedings to ensure there is a sufficient deterrent. Without effective cross border collaboration to bring these criminals to justice fraud is likely to remain the UK's most common crime.

4. **Driving collaboration across industry**

Banks are too focused on their efforts to transfer liability for fraud to other industries. This creates a hostile environment which plays into the hands of fraudsters. Instead, the Government should end the blame game and drive collaboration between industries affected by fraud. Meta has led the way on this work through our collaboration with Stop Scams and the Online Fraud Group. Last year in partnership with two financial institutions we launched a pilot of an intelligence sharing scheme we are calling the Fraud Intelligence Reciprocal Exchange (FIRE). This is a global first whereby banks can share live intelligence to help stop fraud and we can use this information to evolve and improve our machine learning and AI detection systems. We need the Government to use its power to convene to encourage more cross-industry collaboration like this.

Fraud reports

User reports are a vital source of intelligence in our fight against fraud. As I outlined during the hearing Meta invests significantly in building protections for the people that use our platform and building barriers to make it as difficult as possible for fraudsters to reach those people. However, fraud is extremely adversarial. Fraudsters constantly change their behaviours, and are directly financially incentivised to do all they can to find ways around the protections we put in place.

When this happens it is vital that users can report something they think is suspicious to us as easily as possible. We use that intelligence to make decisions on removing content which otherwise evades our detection systems and retrain those systems to better detect this content in the future.

Because this intelligence is such a vital weapon in our fight against fraud, we invested in building an easy to use, reporting system across all of our apps. A user can simply click on the three dots at the top right corner of any piece of content or ad across Facebook and Instagram and will be immediately shown an option to report.

We review every report we get from users and if the content which has been reported to us breaches our community standards it will be removed. If it doesn't, we will still use that report as intelligence that this content or ad may be suspicious. That means that even if it doesn't breach our standards we can take action if we receive further reports.

We do not immediately remove content when it is reported if it doesn't breach our standards because we sometimes see the reporting button being used for other purposes. For example, sometimes people report something they don't like or have an issue with - like a politician or celebrity. We therefore need to strike a balance between taking action where we have a suspicion something may not be right and ensuring we don't accidentally take down legitimate content.

Collaboration with law enforcement agencies

As I mentioned during the hearing we work very closely with a number of law enforcement agencies and their responsible government departments including the City of London Police (in their capacity as the country's lead police force on fraud), the National Economic Crime Centre (NECC), the National Crime Agency (NCA) and of course the Home Office.

We meet with the NECC on a biweekly basis to discuss opportunities to work together and are active members of the Online Fraud Group which is run by the NECC. We recently took part in a 'task and finish' working group on Money Mules/Mule herders and as part of this launched the FIRE intelligence sharing scheme with banks. We have also begun a 'task and finish' group on e-commerce scams and look forward to finding similar collaborative solutions to stopping fraud. We also meet with subject matter experts from the National Fraud Intelligence Bureau at the CoLP on a monthly basis to exchange the strategic intelligence picture. Outside of this regular cadence we recently welcomed a group of representatives from across these agencies to our London HQ to share intelligence we had gathered on the crime of pig butchering, who we believed to be behind this activity, and how we could work together to stop these criminals.

We do not proactively share fraud reports with law enforcement because the scale of this data is such that it would be difficult to manage and the usefulness of the data would be limited and possibly unhelpful. As mentioned above, not all fraud reports are genuine and those which are, are rarely clear cut. The nature of fraud means that we are taking decisions on extremely grey areas - fraudulent content is designed to look normal and innocuous, so even where we have taken action to remove content we have done so because it has breached our community standards or because we have a strong suspicion, not because we know it to be fraudulent. This is because we very rarely have visibility of a crime actually taking place in the way that Banks do.

However, whilst we do not proactively share these reports with law enforcement we do respond to requests for information from Law Enforcement regularly and quickly. Last year in the UK we responded to just under 20,000 requests for information from law

enforcement to assist in their investigations, producing data in over 87% of cases. We also have a dedicated reporting portal for law enforcement partners - both to rapidly remove content and to aid with deeper investigations into the serious organised crime gangs behind much of this fraudulent activity.

Finally, we are in active discussions with the City of London Police (CoLP) regarding their efforts to reboot Action Fraud, including how we can work together to use the data that Action Fraud's successor will collect to take action against fraudulent activity on our platforms.

Advertisers who have withdrawn spending

Meta is both directly and indirectly incentivised to do all we can to combat fraud on our platforms. First and foremost the safety and security of the people who use our services is our number one priority. As set out above our business relies entirely on providing a safe and enjoyable experience for people when they use our services and the existence of fraud on our platforms, even if you don't fall victim to it, directly undermines that experience and makes it more likely you will go elsewhere. And the same is true of advertisers, even if your ad doesn't appear anywhere close to fraudulent content the existence of fraudulent ads on our platform undermines trust in advertising. Without those two cohorts, the people who use our platforms and the advertisers who pay to reach those people, we don't have a business, so we have a business imperative to do all we can to combat fraud.

As I set out during the hearing Meta is also directly liable for losses incurred via stolen credit cards used on our services or hacked ad accounts with credit lines which are used by scammers.

As set out here, these risks are not merely reputational but represent real world impact on Meta's bottom line.

Fraudulent financial advice profiles

Meta has developed market leading technology to detect and take action on the creation of fake accounts. In the last quarter of 2023 we removed 827m fake accounts, and we removed 99.1% of those accounts before they were reported to us.

However, we know that fraudsters do sometimes evade this detection, so we have also invested in proactive machine learning tools to scan content for suspicious signals. This can include signals specific to the content itself - when looking for investment scams we look for content which is promising an unreasonably high rate of return, or low risk, high

guaranteed rewards and if we think this content may be fraudulent we remove it. However, because fraud is extremely adversarial we have learnt that it is most effective to combine content level detection with looking for behavioural indicators that we would commonly associate with fraudsters. This is because fraudsters can easily change the content they use but their modus operandi and the tactics they use are far more difficult to mask or change. As a result we also look out for key indicators like accounts which are messaging a large volume of other accounts, or accounts which have received a high rate of negative feedback to help us identify potentially suspicious accounts.

Outside of our detection of potentially fraudulent financial advice being posted organically we have also introduced additional controls to combat fraudulent financial service advertising. In order to advertise financial service products to UK users on Meta platforms you must now first be registered with the FCA and this status is verified before you can advertise.

Facebook Marketplace

Finally, I noted that the committee had a particular interest in Facebook Marketplace during the session so I wanted to take the opportunity to set out some of the specific measures and protections we have in place on Facebook Marketplace here.

Firstly, as I set out during the hearing, Facebook Marketplace is designed to be a one-to-one local listings service which allows people to safely and securely sell and buy items, with payment taking place upon collection. This is why we do not offer the ability to ship an item through Marketplace or to pay on the website itself.

We want Marketplace to be accessible for anyone who wishes to safely and securely buy or sell something; this is why there are no fees for listing products on Marketplace. We do however allow users to pay to boost the visibility of their products if they wish, and these are reviewed against our commerce policies.

We know that fraudsters still try to subvert the way we intend Marketplace to be used and ask people to pay them before they have seen the item, which is why we have taken particular steps to mitigate such a risk. For example, we are introducing prominent warnings in Marketplace inboxes which tell users to never pay for an item without seeing it first. This is a really important way of interrupting the scam at a crucial point and making people think twice about something which otherwise might look legitimate. We have also introduced cross border filtering which means we can combat the risk of someone claiming to have an item for sale in the UK while they are actually based

overseas. As part of our commitments in the online fraud charter we will also be introducing increased levels of verification on marketplace.

Over a number of years Meta has made substantial investments into AI technologies which are used to strengthen our detection of this and other harmful content on the platform and as these technologies continue to advance so will our detection.

I hope this letter addresses the questions you asked me to follow up on and as ever I am available to answer any further questions or speak separately to the committee if that would be helpful.

February 2024