November 13, 2025

Chris Mufarrige
Director of the Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

cc: State Attorneys General offices

Dear Director Mufarrige,

Consumer Reports writes to urge you to take action against Meta for knowingly showing billions of scam advertisements *per day* and for failing to take reasonable efforts to staunch the deluge of fraudulent ads on its websites.

Last week, Reuters published a blockbuster article entitled "Meta is earning a fortune on a deluge of fraudulent ads, documents show."[1] According to Reuters, Meta projects that 10 percent of the company's entire revenue will soon be attributable to ads for illegal goods and scams. This would add up to $16 billion per year, a staggering figure. At the same time, Meta has refused to take remedial steps to curtail the stream of harmful ads, defunding its safety teams and taking action against advertisers in only the most extreme of circumstances.

Under the FTC Act and many state consumer protection laws, companies are prohibited from engaging in "unfair" business practices that cause significant injury, are not reasonably avoidable by consumers, and that are not offset by countervailing benefits to consumers or competition. This includes injuries caused by third parties that a company had the capacity to stop but failed to take reasonable steps to do so. For example, the FTC has brought dozens of enforcement actions against companies for failing to use reasonable security measures to stop attackers from accessing consumers' personal information. Here, the Meta documents reviewed by Reuters showed that Meta was aware of the massive scope of illegal and harmful activity on its platforms and consciously chose to underinvest in measures that could have minimized the harm.

---

[1] Jeff Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, Reuters, (Nov. 6, 2025), https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/. Unless otherwise noted, information about Meta's policies of tolerating fraud on its advertising platform are derived from this article.

In seeking to evade liability, it is possible that Meta will cite to Section 230 of the Communications Decency Act which holds that online platforms are not strictly liable as a speaker for the contents of communications created by another using their platform.[2] However, Section 230 should not insulate Meta from responsibility here. Under an unfairness charge, Meta is not treated as a "speaker" of advertisers' illegal content, rather it is legally responsible for failing to take reasonable steps to protect its users from significant harm — and for its own choices to algorithmically target certain users with ads for fraudulent or illegal products. Section 230 was designed to incentivize platforms to take steps to address third-party abuses; giving Meta blanket immunity for displaying 15 billion fraudulent ads daily would hardly encourage the company to take any steps at all to rein in the worst actors.

Meta appears to have been aware that its facilitation of illegality exposed the company to liability, as it estimated regulatory fines of up to $1 billion related to its delivery of fraudulent and illegal advertisements. While we agree with Meta that it bears legal responsibility here, $1 billion in fines would be an irresponsibly weak response given the profits the company made from such activities. We urge US enforcers to take strong action to hold Meta accountable for its facilitation of fraud and illegal activity at such an unprecedented scale.

I. Meta's Delivery of Billions of Scam Attempts Daily is an Unfair Business Practice

To determine whether Meta has engaged in unfair business practices under the FTC's consumer protection authority, the agency must demonstrate that

> the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[3]

In this case, the first two prongs are easily met: Meta according its own estimates delivers billions of ads for fraudulent or illegal products every single day. Scam ads are designed to fool consumers, depriving them of the ability to avoid the harm. In fact, when users click on fraudulent ads on Meta's platform, Meta's algorithms are designed to target those users with additional fraudulent ads in the future.

Meta's tolerance of fraudulent and illegal ads meets the third prong of unfairness as well, as the company failed to take reasonable, cost-effective steps to cut off even the most egregious abusers. While Meta should not be strictly liable for all illegal activity on its platforms, here documents reviewed by Reuters show that it was aware of the massive scale of the problem and refused to take basic remedial actions to meaningfully address the problem.

---

[2] 47 U.S.C. § 230.
[3] 15 U.S.C. § 45(n).

Significant injury

The first prong of the FTC's test for unfairness under Section 5 is whether the practice caused substantial harm to consumers. The sheer volume of scam advertisements that Meta displays to users, recently reported by Reuters, combined with the company's large user base and its internal estimates of how much fraud it facilitates each year clearly amounts to substantial harm.

Internal documents reported in Reuters indicate that in 2024, Meta estimated its users are seeing an estimated 15 billion "high risk" scam advertisements — the term it uses for ads that show clear signs of being fraudulent — every day.[4] Scammers choose Meta products in part because they give fraudsters access to massive numbers of consumers. In the fourth quarter of 2024, Meta had 3.35 billion active daily users across its family of apps, which include Facebook and Instagram.[5] This would mean that, on average, each Meta user is exposed to roughly 11 scams on a Meta product each day, based on Meta's own estimates of scam attempts. Meta's audience is so large, that even if only a small share of its users fall victim to one of these scams, a large group of consumers are harmed.

This aligns with Meta's own internal estimates. Reuters reported that Meta staff estimated in 2025 that the platform is involved in one third of *all successful scams in the U.S.* This shockingly high estimate is supported by evidence from other countries. According to the U.K.'s independent payments regulator, Meta platforms were linked to 54% of scams in the country in 2023, more than double all other social platforms combined.[6] According to the Federal Trade Commission's 2024 data, scams that start on social media result in the highest overall reported losses, with $1.9 billion reported lost that year.[7] This number is certainly an

---

[4] This shocking number does not represent all scams Meta estimates it facilitates each day. On top of the 15 billion likely fraudulent advertisements, Meta estimates that its users are exposed to an additional 22 billion organic scam attempts every day on its family of products, per internal documents uncovered by Reuters. Organic scams are any scams on Meta that do not include paid advertisement, such as "fraudulent classified ads placed for free on Facebook Marketplace, hoax dating profiles and charlatans touting phony cures in cancer-treatment groups." Reuters offered the example of fraudsters who hacked a user account and began reaching out to that user's friends and contacts with a crypto scam; four of the user's professional contacts were defrauded, with a total loss of at least $46,000.

[5] *Meta Reports Fourth Quarter and Full Year 2024*, Meta Public Relations, (Jan. 29, 2025), https://investor.atmeta.com/investor-news/press-release-details/2025/Meta-Reports-Fourth-Quarter-and-Full-Year-2024-Results/

[6] *Unmasking how fraudsters target UK consumers in the digital age*, Payment Systems Regulator, (Dec. 2024), https://www.psr.org.uk/information-for-consumers/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age/?utm_source=chatgpt.com and https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

[7] Press Release, *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*, Federal Trade Comm'n, (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024?.

undercount; research suggests that fewer than 1% of all scams are reported to a state or federal governmental agency.[8]

Taken together, recent evidence suggests that Meta is one of the most significant engines of fraud in the United States. And, as will be discussed in more detail below (*infra*, *Not offset by countervailing benefits to consumers or competition*), Meta was aware of the scale of this fraud and deliberately underresourced efforts to curtail it.

Unavoidable by consumers

The second prong of the FTC's unfairness test is whether consumers could reasonably avoid the harm. Longstanding FTC guidance establishes that in order for a consumer to be able to reasonably avoid harm, they must be able to make a free and informed choice.[9] When actors are intentionally attempting to deceive consumers, they are deprived of that informed choice.

Here, scammers inundated Meta with fraudulent content designed to fool consumers into parting with their money. Even savvy and sophisticated consumers could easily fall victim to one of the billions of deceptive ads shown on the platform. Meta's ad-targeting system exacerbated the problem, as Meta users who clicked on one scam ad were likely to be shown more scam ads thanks to the company's ad-personalization algorithms, which attempt to show users more ads like ones they've interacted with. Thus, if someone is particularly vulnerable to scams, Meta's algorithm ensures those scam ads are unavoidable.

Lastly, consumers could not reasonably avoid harm because Meta concealed from the public just how common scams are on its platforms. Until Reuters' recent reporting, the public had an extremely limited understanding of just how prevalent fraud is on Meta platforms. Recent reporting also suggests that Meta's systems for consumers to report frauds and scams are largely illusory. Safety staffers at Meta estimated in 2023 that users on Facebook and Instagram were submitting around 100,000 valid reports of attempted fraud each week, but that the company "ignored or incorrectly rejected" 96% of them. Taken together, consumers couldn't reasonably make an informed decision about the risks of using Meta's platforms, because the scale of Meta's scam problem was hidden, and they also did not know that the systems for handling fraud reports were largely ineffective in practice.

Not offset by countervailing benefits to consumers or competition

The final prong of the FTC's unfairness test is whether the injury to consumers is outweighed by any offsetting consumer or competitive benefits that the practice also produces. As established above, the injury to consumers from Meta's permissive approach to scam advertisements is massive — therefore the countervailing consumer or competitive benefits

---

[8] Keith B. Anderson, *To Whom Do Victims of Mass-Market Consumer Fraud Complain?*, SSRN, (MAy 24, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323.
[9] *FTC Policy Statement on Unfairness*, appended to *In re International Harvester Co.*, 104 F.T.C. 949, 1070–76 (1984).

would need to be considerable. However, Meta is also a giant, interconnected set of platforms where some degree of fraud is inevitable, and if the cost to remediate fraud and scams — which would to some extent be passed down to consumers in the form of delayed features or more advertisements — outweighed the diminishment of fraud attempts, there would be no unfairness under Section 5. In this case, however, it is more than evident that Meta failed to take the most cursory, cost-effective steps to stop even the biggest known fraudulent actors.

The documents reviewed by Reuters show that Meta was aware as of 2024 that it would earn more than 10% of its revenue from scams and other prohibited ads. Meta was also aware of the fact that it was particularly easy to advertise scams on its services compared to competitors and that their scam prevention policy was underinclusive in obvious ways.[10] Much of this appears to be related to the high bar Meta set for banning advertisers — Meta only took action when they were 95% certain that advertisers were committing fraud. When they were less certain — but still viewed the advertiser to likely be scamming users — they simply charged that advertiser a higher price. Meta employees also documented egregious examples of scams that would not violate Meta's policy, such as a crypto scam featuring a fake account purporting to belong to the Prime Minister of Canada, and ads flagged by the Singaporean police that included "too good to be true" offers of 80% off a designer fashion brand, promotions for fake concert tickets, and job ads posted by entities falsely claiming to be major tech companies. Moreover, even when scammers were caught, they were often allowed to violate Meta's policy several times over before facing adverse action. Multiple accounts earning Meta's internal designation of "Scammiest Scammer" of the month were not shut down until Reuters flagged them during the reporting of its story. As noted above, Meta failed to follow up on 96% of valid complaints about scams according to the company's own employees.

Meanwhile, Meta actively weighed the cost of reducing scams against the likely regulatory fines stemming from this self-described "violating revenue," but concluded that the fines would pale in comparison to the profits, according to the documents reviewed by Reuters. Ultimately, Meta executives only decided to make moderate reductions to the amount of revenue attributable to scams. In fact, according to the Reuters investigation, Meta had an internal policy that prevented the team responsible for vetting advertisements from taking actions that would cost Meta more than .15% of its total revenue.

Meta's net margins have ranged from 15-30 percent over the last several years,[11] with recent dips reportedly attributable to massive spending on AI infrastructure build-out.[12] Even as it spends tens of billions of dollars on data centers ($70 billion in 2025 alone), Meta could dramatically reduce its revenue from scam ads and still remain a wildly profitable company. Instead, it has chosen to make minor tweaks along the margins and act only in instances of

---

[10] For example, according to one internal assessment in April of 2025, "It is easier to advertise scams on Meta platforms than Google."
[11] *FB Financial Profit Margin 2014-2025 | FBK*, Macrotrends, https://www.macrotrends.net/stocks/charts/FBK/fb-financial/profit-margins.
[12] *Nauman Khan, Meta Stock Dips as AI Spending Hits Margins, Triggers Short-Term Selloff*, Yahoo! Finance, (Nov. 5, 2025), https://finance.yahoo.com/news/meta-stock-falls-ai-spending-113904029.html.

impending regulatory intervention. Indeed, safety staffers were explicitly told not to limit their use of Meta's computing resources, instead being directed to "just keep the lights on."

This evidence strongly suggests that Meta's tolerance of scam advertisements on its platforms is not an unavoidable tradeoff, it is a profit-driven policy choice. But it is also an unfair business practice that has led to substantial harm, was not avoidable by consumers, and which was not offset by countervailing benefits to consumers or competition.[13]

II. Meta is Not Insulated from Liability by Section 230 of the Communications Decency Act

In failing to take action to protect its users from rampant scams and illegal solicitations on its platforms, Meta should not be insulated from liability by Section 230 of the Communications Decency Act. In general, Section 230 holds that online platforms should not be considered the speaker or publisher of content that it simply hosts on behalf of another entity. For example, if a user were to post defamatory material to X.com, Section 230 provides that X would not be held liable as a publisher for such content. In at least one jurisdiction, Meta has successfully (in part) used Section 230 to defend itself from actions seeking to hold the company liable for the content of certain advertisements.[14]

---

[13] In addition to an unfairness claim, Meta may be liable for deceptive practices under the FTC's and states' unfair and deceptive practices authority. Facebook has long promised in its Terms of Service to protect consumers from "harmful conduct" on its services, (*see Terms of Service*, Archive.org capture of Facebook, (archived on Feb. 2, 2022), https://web.archive.org/web/20220202002659/https://www.facebook.com/terms/) and Meta's Community Standards claim that Meta will remove content and combat behavior "that purposefully employs deceptive means - such as wilful misrepresentation, stolen information and exaggerated claims - to either scam or defraud users and businesses." *Fraud, Scams, and Deceptive Practices*, Facebook, https://transparency.meta.com/policies/community-standards/fraud-and-scams/. In reality, Meta was doing little to proactively combat scams and respond to credible user reports of scams. According to documents obtained by Reuters, Meta's policy was only to ban advertisers when they were 95% certain that they were committing fraud. In a recent class action suit over fraudulent ads served on the site, while the court held that Section 230 barred some of plaintiffs' claims (*see* Section II, *infra*), the court refused to dismiss contract claims that Meta failed to moderate third-party advertisements as promised in its terms of service. *Calise v. Meta Platforms, Inc.*, No. 22-15910 (9th Cir. 2024), https://cdn.ca9.uscourts.gov/datastore/opinions/2024/06/04/22-15910.pdf.

[14] *Calise v. Meta Platforms, Inc.*, No. 22-15910 (9th Cir. 2024), https://cdn.ca9.uscourts.gov/datastore/opinions/2024/06/04/22-15910.pdf. Both *Calise* and a district court ruling against the FTC against Match.com weigh in favor of a finding of Section 230 immunity for Meta. *FTC v. Match Group, Inc.*, No. 3:19-CV-2281-K (N.D. Tex. March 24, 2022). However, these opinions are inconsistent with the general body of caselaw on unfairness authority and third-party harm, as well as recent decisions holding social media companies liable for algorithmic targeting of harmful content, discussed below. In addition, while some of the FTC's charges against Match.com were dismissed, others survived a motion to dismiss, and the company recently agreed to a $14 million settlement to resolve them. *See* Press Release, *Match Group Agrees to Pay $14 Million, Permanently Stop Deceptive Advertising, Cancellation, and Billing Practices to Resolve FTC Charges*, Fed. Trade Comm'n., (Aug. 12, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/08/match-group-agrees-pay-14-million-permanently-stop-deceptive-advertising-cancellation-billing.

A Section 5 unfairness claim however does not seek to hold Meta liable as a publisher or speaker of fraudulent content. Rather, it argues that a company has failed to take cost-effective steps to protect users from the reasonably foreseeable harm caused by another.

Unfairness law requires platforms to exercise a reasonable degree of diligence to stop bad actors

The FTC has long held that companies' failure to take action to identify and remediate harmful uses by bad actors of their products will in many cases be an unfair business practice. One analogous line of cases is the FTC's enforcement actions on data security. In nearly a hundred cases since 2005, the FTC has said that companies have a legal obligation to anticipate and respond to ways that attackers could misuse their systems to gain access to consumers' personal information.[15] In these cases, the FTC has said that companies' failure to take steps to remediate likely abuses by third parties caused a substantial likelihood of injury that was unavoidable by consumers and not offset by countervailing benefits to consumers or competition. As just one example, last year, the FTC brought an action against the security camera company Verkada for failure to take steps to prevent attackers from accessing video feeds from consumers' cameras.[16]

Beyond data security, the FTC has held companies responsible for how others use their products to cause harm to consumers.[17] For example, the FTC successfully sued QChex for violating Section 5 for allowing any customer to create checks for any bank account number without implementing reasonable safeguards to ensure that fraudsters were not creating checks

---

[15] *See* Press Release, *BJ's Wholesale Club Settles FTC Charges*, Fed. Trade Comm'n., (Jun. 16, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; Press Release, *DSW Inc. Settles FTC Charges*, Fed. Trade Comm'n., (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges; Press Release, FTC Releases 2023 Privacy and Data Security Update, Fed. Trade Comm'n., (Mar. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update; Staff Report, Start with Security: A Guide for Business, Fed. Trade Comm'n, (Jul. 2017), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[16] *See* Press Release, *FTC Takes Action Against Security Camera Firm Verkada over Charges it Failed to Secure Videos, Other Personal Data and Violated CAN-SPAM Act*, Fed. Trade Comm'n., (Aug. 30, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-takes-action-against-security-camera-firm-verkada-over-charges-it-failed-secure-videos-other.

[17] *See*, *e.g.*, Press Release, *FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions*, Fed. Trade Comm'n, (Jun. 28, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-sues-walmart-facilitating-money-transfer-fraud-fleeced-customers-out-hundreds-millions; Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement*, Fed. Trade Comm'n, (Oct. 4, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network-responsible-deceptive-third-party-claims. Press Release, *Court Orders Permanent Halt to Illegal Qchex Check Processing Operation Court Finds Qchex Unfair Practices Created a Dinner Bell for FraudstersOperators to Give Up All Their Ill-Gotten Gains*, Fed. Trade Comm'n, (Feb. 9, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/02/court-orders-permanent-halt-illegal-qchex-check-processing-operation-court-finds-qchex-unfair.

for accounts they did not control. In that case, QChex's failure to take steps to prevent foreseeable harmful and illegal uses constituted an unfair business practice.

It is important to note that an obligation to identify and remediate likely harmful behaviors does not amount to strict liability for any harm caused by another bad actor using a company's product.[18] Section 5's requirement that any harm not be offset by countervailing benefits to consumers or competition means that companies are not expected to spend unlimited resources to try to chase down potential offenders. Instead, the FTC only intervenes when companies fail to take cost-effective measures whose implementation would have prevented an even greater risk of injury. In this case, Meta should not be strictly liable for the fraud caused by online advertisements, but only for failing to take commercially reasonable steps to limit the amount of fraudulent content in the advertisements on its platforms.

In this case, however, it is clear that Meta deliberately failed to take even rudimentary actions to address the billions of scam advertisements that it was showing its users every day. As such, Meta should be liable — not as a speaker of the fraudulent advertisements — but for failing to take reasonable steps to remediate the harm caused by illegal advertisements running on the Meta platform.

Section 230 was enacted in large part to eliminate a perverse incentive created by some early internet-era court decisions which held that any good-faith company efforts to remediate harms opened the company up for liability for such harms by demonstrating awareness of them.[19] Granting Section 230 immunity in a case such as this, however, would create its own perverse incentive where it is unquestioned here that Meta was aware of fraud at an almost unprecedentedscale taking place on its platform. Consumer protection law has been used for decades to require platforms to take actions to stop fraudsters from harming users — platforms should not get a get-out-of-jail free card to absolve themselves from their responsibility to remediate third-party harm just because the harm is speech-based (as opposed to other cybersecurity attacks such as credential stuffing and malware).

Meta is not just hosting fraudulent content, its algorithms are optimizing for it

Further, Meta is not merely passively hosting internet content — it is taking money to place ads and using its proprietary algorithm to target users with particular ads. As reported by Reuters, Meta served users who had previously clicked on fraudulent ads with *more* fraudulent ads, since Meta's algorithms were designed to show users content with which they were more likely to engage. In recent years, several cases have denied Section 230 immunity to online platforms in lawsuits that accused the company of algorithmically prioritizing certain content. For example, in *Lemmon v. Snap*, Snap was unable to dismiss a cause of action against the

[18] However, it is worth noting that in some other legal contexts, online platforms may be deemed strictly liable for harms caused by third-party use of their systems. For example, in the product liability context, platforms such as Amazon that host third-party sellers of defective products may be held strictly liable for the damages caused by those products. *See Oberdorf v. Amazon.com Inc.*, 930 F.3d 136 (2019).
[19] S*tratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995).

company over the company's algorithm overindexing on content glamorizing risky and illegal behavior.[20] Similarly, in *Anderson v. TikTok*, a court dismissed a Section 230 challenge to TikTok's immunity because the speech in question — TikTok's algorithmic feed — was clearly within the control of TikTok itself. That case in turn cited the recent Supreme Court decision in *Moody v. NetChoice LLC* which held that a company's "editorial judgments" about "compiling the third-party speech it wants in the way it wants" is the platform's own "expressive product" — that is, not the speech of someone else, and not insulated from accountability by Section 230.

As such, even if a court were to deem that Meta were not responsible for *hosting* fraudulent ads because of Section 230 — despite awareness of widespread fraud and failure to take reasonable steps to protect its users from harm — it should still hold Meta liable for designing its algorithm to *target* users with such ads.

III. Conclusion

Meta seems to recognize it has substantial legal liability for turning a blind eye to pervasive fraud on its platform: according to the Reuters article, "Meta has internally acknowledged that regulatory fines for scam ads are certain, and anticipates penalties of up to $1 billion, according to one internal document."

However, given Meta's massive revenues — much of which is directly attributable to fraud — a fine of one billion dollars would be insufficient in this case to account for the harm that Meta has caused consumers and to deter Meta from similar behavior going forward.

We urge the FTC and state attorneys general to take strong action to hold Meta accountable for its facilitation of fraud and illegal activity at such an unprecedented scale. Please reach out to justin.brookman@consumer.org if there is anything Consumer Reports can do to assist in this matter.

Respectfully,

Justin Brookman
Director, Technology Policy

Matt Schwartz
Policy Analyst

[20] *Lemmon v. Snap Inc.*, 995 F.3d 1085 (9th Cir. 2021).

Grace Gedye
Policy Analyst