



November 22, 2025

VIA EMAIL

Andrew N. Ferguson
Chairman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

Paul S. Atkins
Chairman
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Dear Chairman Ferguson and Chairman Atkins,

We write to urge the Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC) to investigate and, if appropriate, bring enforcement actions against Meta for its facilitation of and profiting from criminal investment scams, fake government benefits schemes, deepfake pornography, and other fraudulent activities.

According to recent reporting from Reuters, internal documents show that Meta has earned billions of dollars from fraudulent and scam advertising while internally stifling measures to prevent fraud. By its own assessment, 10% of Meta's annual revenue for last year was generated from scam advertisements, a windfall of \$16 billion in one year alone.¹ Meta's central, facilitating role in scams against consumers is unprecedented: by its own employees' assessment, Meta was involved in one-third of all successful scams in the US and was unmatched by other Big Tech platforms. Using the FTC estimate of \$158.3 billion in overall fraud per year, this would suggest Meta was responsible for more than \$50 billion in consumer loss last year.² This internal finding supports a December 2024 report by a U.K. financial regulator that found Meta's platforms (Facebook, Instagram, and WhatsApp) were linked to 54% of payment scams and a JPMorgan

¹ Jeff Horwitz, *Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show*, REUTERS (Nov. 6, 2025, 6:00 AM), <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06>.

² FED. TRADE COMM'N, PROTECTING OLDER CONSUMERS 2023–2024 (2024), www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf.

Chase investigation that found Meta accounted for nearly half of all reported scams on Zelle, such as romance scams that feign a love interest to deceive a victim and fake investment schemes.³

Meta's ill-gotten gains appear to be no accident: it has made conscious choices based on business considerations that turned a blind eye and enabled it to profit from illicit advertisements. According to Reuters, Meta had "specific revenue guardrails" that blocked its anti-fraud team from taking action that would cost Meta more than even a mere 0.15% of the company's total revenue. In line with that approach, Meta only bans advertisers if its automated systems predict the marketers are all-but- certain to be committing fraud and by its own estimates, it has ignored or incorrectly rejected 96% of user reports of fraud. Moreover, perversely, Meta reportedly charges higher rates for ads that it suspects might be fraudulent — in effect, imposing a scam tax that provides an additional lucrative revenue stream that it knows is tied to fraud. Further, because Meta's advertising algorithms targets individuals based on their past clicks and interest, a person that falls for a scam is more likely to be targeted by even more scams or fraudulent advertising — making Facebook and Instagram a fraud trap that can repeatedly exploit vulnerable individuals. Meanwhile, these scams have been allowed to take over Facebook and Instagram as Meta has drastically cut its safety staff, including for FTC mandated reviews,⁴ even as it dumps unimaginable sums into its generative AI projects.

As it does every time its abuses and failures are discovered, Meta has repeatedly claimed it is cleaning up its act — but there is overwhelming evidence it continues to knowingly profit from fraud. Even a short review of Meta's Ad Library at the time of this letter⁵ shows clearly identifiable advertisements for illicit gambling,⁶ payment scams,⁷ crypto scams,⁸ AI deepfake sex services,⁹ and fake offers of federal benefits,¹⁰ advertisements that often falsely appear to link to legitimate sites. Further, despite the company's rules against nudity, advertisements for pornographic and sexually explicit material,¹¹ and which often lead to malware, are widespread on Meta's products. While Meta has been warned about advertisement deepfakes impersonating

³ PAYMENT SYS. REGUL., UNMASKING HOW FRAUDSTERS TARGET UK CONSUMERS IN THE DIGITAL AGE (2024), <https://www.psr.org.uk/media/u0vnqlra/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age-dec-2024.pdf>; Jeff Horwitz & Angel Au-Yeung, *Meta Battles an "Epidemic of Scams" as Criminals Flood Instagram and Facebook*, WALL ST. J. (May 15, 2025, 9:00 PM), <https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8>.

⁴ Jonathan Vanian, *Meta Replacing Humans with AI for FTC-mandated Privacy Reviews*, CNBC (Oct. 23, 2025, 5:57 PM), <https://www.cnbc.com/2025/10/23/meta-replacing-humans-with-ai-for-ftc-mandated-privacy-reviews.html>.

⁵ The advertisements associated with advertiser identifiers may include content that is sexually explicit, fraudulent, or malicious, and may not be suitable for viewers. A copy of the pages will be kept on record for the Commission.

⁶ Advertiser ID: 122101083962009471.

⁷ Advertiser ID: 106883315517534.

⁸ Advertiser ID: 768957359643372.

⁹ Advertiser ID: 742415435615152.

¹⁰ Advertiser ID: 100942582690100.

¹¹ Deimantė Karaciejūtė, *Like, Share, and Beware: Facebook Infested with Porn and Gambling Ads*, CYBERNEWS (Jan. 22, 2025), <https://cybernews.com/editorial/pornographic-ads-on-facebook>; Emanuel Maiberg, *Facebook Is Censoring 404 Media Stories About Facebook's Censorship*, 404 MEDIA (Jan. 8, 2025, 9:00 AM), <https://www.404media.co/facebook-is-censoring-404-media-stories-about-facebooks-censorship>.

politicians,¹² it still continues to run fraudulent clips, including President Trump claiming to offer a “\$1,000 Snap replacement program” — preying on the most vulnerable in America.¹³ The beneficiaries of these scams are often cybercrime groups based in China, Sri Lanka, Vietnam and the Philippines.¹⁴

The reporting makes clear that Meta will not act on this rampant fraud and criminality unless the FTC and SEC put an end to it. According to Reuters, Meta executives actually limited their anti-fraud enforcement efforts to focus only on “countries where it feared near-term regulatory action.” In line with these efforts, in anticipation of enforcement, Meta had budgeted for penalties of up to \$1 billion, which were a mere fraction of the \$7 billion in annual revenue from high-risk advertisement alone.

The FTC and SEC should immediately open investigations and, if the reporting is accurate, pursue vigorous enforcement action where appropriate to force Meta is fully disgorge all profits from fraudulent advertisements, impose steep civil penalties, hold individual executives personally accountable, and seek binding terms to end this scourge on consumers, our economy, and our national security.

Thank you for your attention to this matter.

Sincerely,



Richard Blumenthal
United States Senator


Josh Hawley
United States Senator

¹² Steven Lee Myers, *Spam and Scams Proliferate in Facebook’s Political Ads*, N.Y. TIMES (Oct. 1, 2025), <https://www.nytimes.com/2025/10/01/technology/facebooks-political-ads-deepfakes-scams.html>.

¹³ Advertiser ID: 128468240345577.

¹⁴ Horwitz & Au-Yeung, *supra* note 3.