

Congress of the United States

Washington, DC 20515

October 16, 2025

Mr. Mark Zuckerberg
Chief Executive Officer
Meta Platforms, Inc.
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

We write to express our deep concern that Meta is profiting from fraudulent political advertisements on Facebook that use artificial intelligence (AI) generated deepfakes and deceptive content to scam consumers.¹ These ads are not just misleading, they are harmful. They trick Americans into handing over money or personal information, while undermining public trust in our institutions and degrading the integrity of our democracy.

According to a recent investigation, advertisers on Meta platforms have engaged in deceptive or fraudulent practices.² They purchased nearly 150,000 ads, spending almost \$49 million over the past seven years. Many of these ads relied on fabricated videos impersonating public officials to promote fake government programs. These scams are designed to deceive everyday Americans, and Meta has continued to profit from them.

The rapid rise of AI and deepfake technology has only made it easier for bad actors to produce fraudulent, hyper-realistic content at scale. Older Americans and other vulnerable communities are particularly at risk. The Federal Trade Commission (FTC) reports that scams impersonating government officials and businesses have increased fourfold since 2020, with social media now serving as one of the most common vehicles. Yet despite explicit policies against impersonation and scams, Meta has allowed repeat offenders to continue advertising and generating revenue on its platform.

Congress and the Trump Administration have taken action to address threats, recently through the TAKE IT DOWN Act, legislation we led that underscores the urgent need for stronger protections against the misuse of deepfakes.³ While guardrails are critical, Meta has a responsibility to protect its users today.

¹ Myers, S.L. "Spam and Scams Proliferate in Facebook's Political Ads." *New York Times*. 1 Oct. 2025. Retrieved from: <https://www.nytimes.com/2025/10/01/technology/facebooks-political-ads-deepfakes-scams.html>.

² "Meta Awash in Deepfake Scam Ads." *Tech Transparency Project*. 1 Oct. 2025. Retrieved from: <https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads>.

³ Congresswoman Debbie Dingell. *Press Release: Dingell's TAKE IT DOWN Act Signed into Law*. 19 May 2025. Retrieved from: <https://debbiedingell.house.gov/news/documentsingle.aspx?DocumentID=5763>.

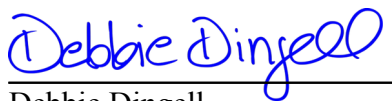
We request written responses to the following questions to better understand how Meta intends to address these issues:

- What steps is Meta taking to protect vulnerable users from AI-driven scam ads and impersonation?
- Does Meta notify individuals who have been exposed to fraudulent or deepfake ads? If not, why not?
- What technology and review processes does Meta use to detect deepfakes before they run as ads?
- How many political ads flagged as deepfakes or impersonations were allowed to run before removal in the past 12 months?
- Why were repeat violators permitted to continue advertising, and how much revenue has Meta derived from such advertisers since 2020?
- What enforcement mechanisms does Meta impose when advertisers violate policies against fraudulent or deepfake content?
- What resources or staff has Meta dedicated to ensuring its advertising review system can keep pace with evolving AI-generated threats?

This conduct leaves Meta's users exposed, undermines consumer trust, and raises serious questions about whether your company is prioritizing profit over protection in the age of AI.

Thank you for your attention to this matter, and we look forward to your response.

Sincerely,



Debbie Dingell
Member of Congress



August Pfluger
Member of Congress