



Testimony on Pennsylvania Informational Hearing on Scams

February 25, 2026

Chairman Ryan Bizzarro and Members of the House Democratic Policy Committee, thank you for the opportunity to submit written testimony on the growing harm of tech-enabled scams and their impact on Pennsylvanians.

In a nationally representative CR survey of 2,158 US adults in April 2025, close to half (46%) of Americans have personally encountered a digital scam attempt or cyberattack. Alarmingly, one in five of them—about one in ten Americans overall—say they lost money to the scam.¹

Americans lose substantial amounts of money due to fraud and scams. In 2023, the Federal Trade Commission received fraud claims from more than 2.6 million individuals. The commission estimated that \$10 billion had been lost that year alone. This figure does not include scams that victims chose not to report.²

Some communities are particularly vulnerable to digital scams. Consumer Reports' nationally representative survey data shows that, among those who had encountered a scam attempt, households with the lowest incomes were three times as likely to report financial losses due to scams as the highest income households (29 percent compared with 10 percent). And we found continued racial disparity in financial losses related to scams. Our data shows that 37 percent of Black Americans who encountered a

¹Noemi Altman, Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults, April 2025,

https://article.images.consumerreports.org/image/upload/v1744212505/prod/content/dam/surveys/Consumer_Reports_AES_April_2025.pdf,

²Federal Trade Commission, As Nationwide Fraud Losses Top \$10 Billion in 2023, FTC Steps Up Efforts to Protect the Public, February 9, 2024,

<https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public>

scam lost money to it, compared to only 15 percent of white Americans.³ This echoes similar findings made by other organizations, including the Federal Trade Commission.⁴

Scammers use insidious strategies to target their victims. Not only can they easily access personal data on individuals, they are now using new methods such as voice cloning and deepfakes to impersonate CEOs, celebrities, banks, government agencies, and people their victims know and trust to get them to lower their guard and open their wallets.⁵

Text-messaging scams are surging, particularly among young people, where the share reporting these types of scam attempts roughly tripled between April 2024 and April 2025, from 13 percent to 40 percent.⁶

Bad actors are exploiting platforms people use regularly to scam and defraud them. For example, a *Reuters* investigation revealed that Meta — according to its own documents — delivered an estimated 15 billion scam ads a day to its users in 2024.⁷ Meta, which operates Facebook and Instagram, failed to identify and remove most scam ads. This exposed billions of users to fraudulent e-commerce scams and investment schemes. Allowing the proliferation of these scam advertisements led to billions of dollars in profit for the corporation. Meta has refused to take remedial steps to curtail the stream of harmful ads, defunding its safety teams and only taking action against advertisers in the most extreme of circumstances.

Online scams proliferate on other platforms as well. YouTube channels have distributed malware by promoting pirated games, often bundled with keyloggers⁸. Additionally, companies have failed to implement meaningful safeguards against the use of their technology. A recent Consumer Reports assessment of AI voice cloning products found that the majority of companies assessed made it

³Noemi Altman, Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults, April 2025, https://article.images.consumerreports.org/image/upload/v1744212505/prod/content/dam/surveys/Consumer_Reports_AES_April_2025.pdf

⁴Federal Trade Commission, *Serving Communities of Color A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color*, October 2021, https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf

⁵Derek Kravitz, *The New Scams to Watch Out For*, Consumer Reports, January 30, 2025,

<https://www.consumerreports.org/money/scams-fraud/new-scams-to-watch-out-for-a9334297641/>

⁶Noemi Altman, Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults, April 2025, https://article.images.consumerreports.org/image/upload/v1744212505/prod/content/dam/surveys/Consumer_Reports_AES_April_2025.pdf

⁷Jeff Horowitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, November 6, 2025, <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/>

⁸Jonathan Greig, *YouTube channels found using pirated video games as bait for malware campaign*, April 3, 2024, <https://therecord.media/youtube-infostealer-campaign-cracked-pirated-video-games>

alarmingly easy to clone a voice without permission, requiring nothing more than a simple checkbox “self-attestation” to claim consent. These companies have failed to implement technical mechanisms to confirm the actual consent of speakers, or to detect and prevent the unauthorized creation of clones based on the voices of public figures, such as celebrities and politicians.⁹

This failure to prevent foreseeable abuse mirrors the Federal Trade Commission’s recent case against the generative AI company Rytr, which sold a service specifically designed to generate a high volume of misleading consumer reviews based on extremely limited prompts¹⁰. The product was easily gameable by bad actors seeking to supercharge scams and skew public perception through the creation of deceptive reviews at scale.¹¹

Online scams are a massive problem for consumers and persist as a source of significant harm due to a lack of consequences for the platforms that tolerate fraudulent ads and even benefit financially from ad fees. While policymakers should enact additional protections to clarify platform responsibilities, they should also utilize existing laws to hold them responsible for failing to take reasonable steps to protect consumers.

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. We urge enforcement agencies to hold platforms accountable for the facilitation of fraud and illegal authority, which causes substantial harm to consumers.

Companies should take commercially reasonable steps to limit the amount of fraudulent content in the advertisements on its platforms, such as

- Collecting and verifying the legal names, business entities, and physical location of advertisers along credit card information as a basic know-your-customer practice so that fraudulent ads can be traced back to specific users.

⁹Grace Gedye, AI Voice Cloning Report, Consumer Reports, March 10, 2025, <https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf>

¹⁰Note that The Federal Trade Commission recently reversed course on the Rytr settlement and dismissed it (FTC Reopens and Sets Aside Rytr Final Order in Response to the Trump Administration’s AI Action Plan, December 22, 2025. <https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-reopens-sets-aside-rytr-final-order-response-trump-administrations-ai-action-plan>)

<https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-reopens-sets-aside-rytr-final-order-response-trump-administrations-ai-action-plan>

¹¹Justin Brookman, Matt Schwartz, Grace Gedye, Rytr Comment to the Federal Trade Commission, November 4, 2024,

https://advocacy.consumerreports.org/wp-content/uploads/2024/11/FTC-2024-0041-0007_attachment_1.pdf

- Investing in measures that could minimize harm, such as impersonation detection and mitigation programs and fraudulent ad detection systems
- Tools for consumers to report suspected fraudulent or deceptive ads, with both automated and manual support
- A timeline for investigating and responding to fraudulent complaints and removing the fraudulent or deceptive ad
- Recourse for buyers and sellers if transactions go awry due to a fraudulent ads or individuals impersonating companies

Thank you for your work on this issue. We look forward to working with you to ensure that Pennsylvania consumers have the strongest possible protections against scam and frauds.

Yael Grauer,
Program Manager, Cybersecurity Research
Consumer Reports