Consumer Federation of America

1620 I Street NW
Suite 200
Washington, DC
20006

202-387-6121
info@consumerfed.org
ConsumerFed.org

PREPARED TESTIMONY AND STATEMENT

FOR THE RECORD OF

Ben Winters
Director of AI and Privacy
Consumer Federation of America

"Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps"

Before The
U.S. House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

Submitted June 2, 2025

I. Introduction

Chair Guthrie, Ranking Member Pallone, Chair Palmer, Ranking Member Clarke and Members of the Subcommittee, thank you for inviting me to testify before you on this important issue. I'm Ben Winters, Director of AI and Privacy at the Consumer Federation of America (CFA). CFA is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Our members include over 200 local, state, and national non-profit groups and consumer protection agencies.

There is a staggering amount of monetary and emotional harm caused by scams perpetrated through robocalls and robotexts. The FBI reports the amount of money lost from internet crime alone surpassed $16 billion last year, rising 33% between 2023 and 2024.[1] According to the Federal Trade Commission (FTC), consumers lost over $12.5 billion to scams last year, an approximately 20% increase from 2023, with sharp increases in lost money for job scams, fake employment agency scams, and investment scams.[2] Truecaller estimates that 60% of scam calls are robocalls.[3] With advanced technologies like AI both increasingly available and unregulated[4], more people are getting texts with personalized scripts written by text generation services and calls with voices that *sound* like their loved ones.[5]

Even when no money is lost, there is a constant sense of annoyance and need for vigilance when people are just trying to live their lives. One figure from the

---

[1] *FBI Releases Annual Internet Crime Report*, April 23, 2025, Federal Bureau of Investigation. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[2] *Top scams of 2024*, March 10, 2025, available at https://consumer.ftc.gov/consumer-alerts/2025/03/top-scams-2024

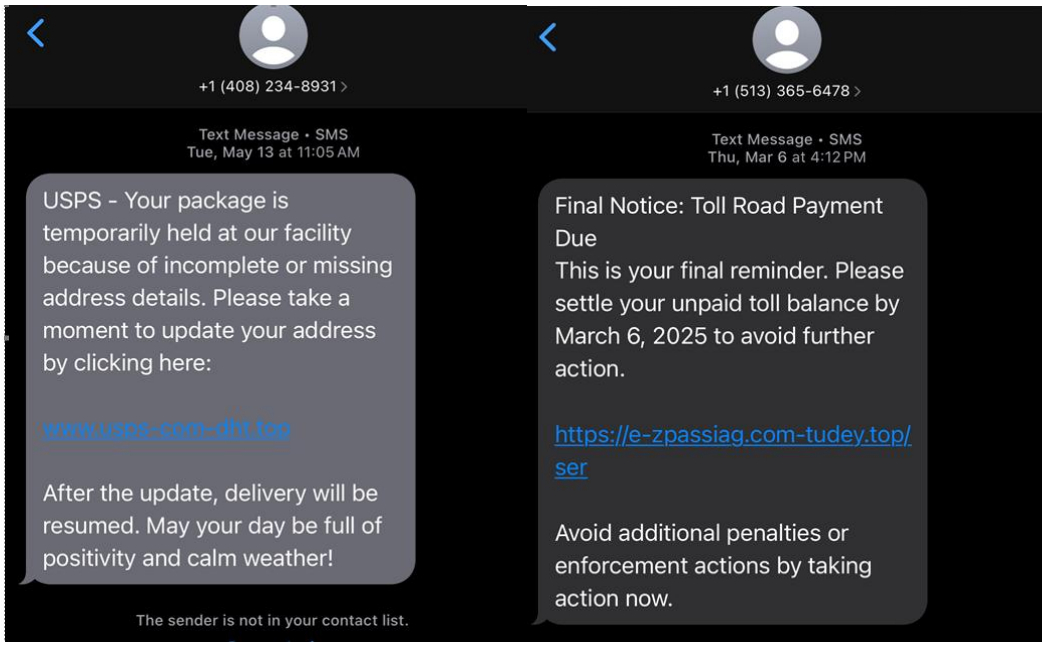
[3] *Id*

[4] Ben Winters, Scamplified · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).

[5] Charles Bethea, The Terrifying A.I. Scam That Uses Your Loved One's Voice, The New Yorker, Mar. 7, 2024, https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice (last visited May 31, 2025).

company Robokiller estimates that 19.2 billion spam robotexts were received by Americans in April 2025 alone.[6]

Americans from all over will recognize messages from scammers purporting to be EZ-Pass[7] or the United States Postal Service[8] and the annoyance, fear, or monetary loss they caused. These are real examples of those messages I've



personally received recently:

An October 2024 Federal Communications Commission (FCC) article shared that Americans are receiving 4 billion robocalls per month, and that "advancements in technology make it cheap and easy to make massive numbers of robocalls and to 'spoof' caller ID information to hide a caller's true identity."[9] This spoofing is what

[6] United States Spam Text Trends and Insights, Robokiller, https://www.robokiller.com/spam-text-insights#introduction (last visited May 31, 2025).
[7] Bill Chappell, (Don't) Click Here to Pay Your Tolls: How You Can Stop Spam Texts, NPR, Mar. 13, 2025, https://www.npr.org/2025/03/13/nx-s1-5326090/dont-click-here-to-pay-your-tolls-how-you-can-stop-spam-texts-smishing (last visited Jun 1, 2025).
[8] Smishing: Package Tracking Text Scams – United States Postal Inspection Service, https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams (last visited Jun 1, 2025).
[9] Robocall Response Team: Combating Scam Robocalls & Robotexts, Federal Communications Commission, https://www.fcc.gov/spoofed-robocalls (last visited May 31, 2025).

leads to calls or texts that look like they're coming from *your* area or from the number of a more official source.[10]

Scammers thrive on chaos and fear like the risk of an unpaid bill or lost package to trick people into engaging with fraudulent offers or revealing sensitive information. They also capitalize on specific current events, such as when scams increase sharply following a natural disaster.[11] We fear that the current increase in regulatory, employment, and economic uncertainty present throughout the country will be a boon for scammers.[12]

These problems are getting worse,[13] and the American people deserve a full court press from Congress and federal consumer protection agencies. Entities responsible for much of the robocall and robotext problem have evaded responsibility for too long.

In this testimony, I will highlight (1) how underregulated technologies including AI are making robotexts and robocalls more effective and easier to make; (2) how federal consumer protection agencies can be doing much more to protect

---

[10] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit*, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025); *Robocall scammers using similar area code to spoof* you, 12WBOY (Apr. 20, 2018), https://www.wboy.com/news/national/robocall-scammers-using-similar-area-code-to-spoof-you/

[11] *See, e.g., Cora Lewis, After Disasters, People Are Especially Vulnerable to Scams. Here's How to Protect Yourself, Associated Press, Jan. 13, 2025, https://apnews.com/article/disaster-identity-theft-scams-a7c2ece38f6c22471f41e00a00d30f0f; After Storms, Watch Out for Scams, Federal Communications Commission, https://www.fcc.gov/consumers/guides/after-storms-watch-out-scams (last visited Jun 1, 2025).*

[12] Isabel Gottlieb, *Regulatory Uncertainty Tops List of Corporate Risks, Survey Says*, Bloomberg Law (Apr. 8, 2025), available at https://news.bloomberglaw.com/us-law-week/regulatory-uncertainty-tops-list-of-corporate-risks-survey-says; Annette Choi and Danya Gainor, *Analyzing the scale of Trump's federal layoffs in his first 100 days*, CNN (Apr. 29, 2025), available at https://www.cnn.com/2025/04/26/politics/federal-layoffs-trump-musk-dg; Talya Minsberg, *A Timeline of Trump's On Again, Off-Again Tariffs*, New York Times (May 26, 2025), available at https://www.nytimes.com/2025/03/13/business/economy/trump-tariff-timeline.html; Abha Bhattarai, *Consumer spending slows as Americans pull back amid tariff uncertainty*, The Washington Post (May 30, 2025). https://www.washingtonpost.com/business/2025/05/30/consumer-spending-tariffs-economy/

[13] YouMail Inc., U.S. Consumers Received Nearly 5 Billion Robocalls in April 2025, According to YouMail Robocall Index, Cision PR Newswire, May 6, 2025, https://www.prnewswire.com/news-releases/us-consumers-received-nearly-5-billion-robocalls-in-april-2025-according-to-youmail-robocall-index-302446599.html (last visited May 31, 2025); Getting more robocalls? Yeah, a lot of us are, U.S. PIRG Education Fund (2023), https://pirg.org/edfund/updates/getting-more-robocalls-yeah-a-lot-of-us-are/ (last visited May 31, 2025)

consumers from robotexts and robocalls; and (3) how Congress can act to protect consumers from this annoying and dangerous problem.

I. Underregulated technologies like AI, data brokers, and call spoofers are making scam problems worse.

A. *Generative AI is a fraudster's dream, and makes scam robotexts and robocalls easier to proliferate and more effective.*

Generative AI, the type of technology behind ChatGPT, ElevenLabs, Sora, and other content creation machines, is one of many types of technologies that facilitate the rise in the scale, accuracy, and plausibility of scams perpetrated through text, phone calls, and other formats.[14]

Generative AI reduces the time and effort criminals must expend to deceive their targets. Generative AI takes what it has learned from examples input by a user and outputs something new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud.[15]

Investment scams, job opportunity scams, romance scams, impersonation scams, and phishing are the exact type that AI can "help" supercharge, and the kind that are rising *rapidly*.[16]

Text-generation tools like Chat GPT make it easier to write phishing attempts, those scams where the bad actor emails or texts something about an order or poses as a loved one or boss to get the recipient to click on something and divulge valuable and personal information by appearing as a trusted source. It also makes it easier to make variations of the same message, which can stymie filters and personalize messages to people easily. Products using text generation tools

[14] Ben Winters, Scamplified · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).
[15] Lana Swartz, Alice E. Marwick, and Kate Larson, ScamGPT: *GenAI and the Automation of Fraud*, Data & Society, https://datasociety.net/library/scam-gpt/ (last visited Jun 1, 2025).
[16] Ben Winters, *Scamplified* · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).

can also create quick and unique human-sounding "scripts" that can be either read by humans or by AI-generated voices.[17]

Filters and other "refusal mechanisms" limit some of the most harmful content, but moderation is inconsistent, inadequate, and unaccountable.[18] For example, Chat GPT refuses to output a phishing text when the prompt is "write a phishing text targeting grandmas," but will return "write an urgent text to my grandma to a grandmother asking her to send me money" to a given website.

These systems also create quicker or more aggressive or simply different variations that would reduce the texts likelihood of getting caught in filters.[19] In CFA's recent "Scamplified" report, we illustrate how easy it is to use ChatGPT to generate over 100 texts with an "urgent ask" to "add 50 dollars' worth of bitcoin to my wallet" (we included a link to a specific bitcoin wallet that ChatGPT's system included in the proposed texts). It was able to customize it with common women's names and include real hospitals in common U.S. cities to create urgency. The system continued to generate significant output texts when we asked it to "target it more to someone that might have dementia."[20]

Between the wide launch of ChatGPT in Winter 2022 and March 2025, there has been a 4151% increase in phishing attacks.[21] A 2021 study completed by Singapore's Government Technology Agency illustrated that phishing attempts made by GPT-3, the model behind ChatGPT, were more successful in tricking receivers into clicking on the email and divulging information than human-made phishing attempts.[22]

---

[17] Electronic Privacy Information Center, Generating Harms: Generative AI's Impact & Paths Forward, (2023), http://www.epic.org/gai (last visited May 31, 2025).
[18] Ben Winters, Scamplified · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).
[19] *Id.*
[20] *Id* at pp. 6-9.
[21] Adaptive Security, Adaptive Security (2024), https://www.adaptivesecurity.com/blog/ai-phishing-chatgpt-impact (last visited May 31, 2025).
[22] Lily Hay Newman, AI Wrote Better Phishing Emails Than Humans in a Recent Test, WIRED, Aug. 7, 2021, http://wired.com/story/ai-phishing-emails/ (last visited May 31, 2025).

Generative AI tools used to carry out robocalls and robotexts don't just stop with text generators, though. Voice cloning tools can now replicate anyone' speech using just a few seconds of audio, often harvested from podcasts, interviews, phone calls, or social media posts like YouTube videos.[23] Scammers have exploited this to impersonate loved ones—such as in "grandparent scams," where a cloned voice mimics a distressed family member to trick victims into sending money.[24] These tools are both accessible and affordable, with platforms like ElevenLabs offering subscriptions starting as low as $5 per month.[25]

According to a report by Consumer Reports earlier this year, major services including ElevenLabs lacked adequate safeguards to prevent misuse and often had weak or nonexistent authentication protocols in place.[26] This means that most platforms offering these services do not require the user to verify their identity or gain consent before creating or using another person's voice or likeness.[27] Single scam calls using these tools are robbing seniors of life savings within minutes.[28]

The FBI warned last year, "These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however,

---

[23] Clare Duffy, AI Voice Scams Are on the Rise. Here's How You Stay Safe. - Terms of Service with Clare Duffy - Podcast on CNN Audio, CNN (2025), https://www.cnn.com/audio/podcasts/terms-of-service-with-clare-duffy/episodes/9fe98d50-96cf-11ef-aa1b-07ca04432229 (last visited May 31, 2025).

[24] Kyle Werner, New Wave of "grandparent" Scams Targeting Elderly Iowans with Fake Calls from Relatives, The Des Moines Register, Jan. 5, 2025, https://www.desmoinesregister.com/story/news/crime-and-courts/2025/01/05/grandparent-scam-iowa-attorney-general-brenna-bird/77454809007/ (last visited May 31, 2025).

[25] Grace Gedye, *AI Voice Cloning Report: Do These 6 Companies Do Enough to Prevent Misuse*, Consumer Reports (2025), https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf (last visited May 31, 2025).

[26] *Id.*

[27] *Id.*

[28] Alvaro Puig, Scammers Use AI to Enhance Their Family Emergency Schemes, Federal Trade Commission (2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes (last visited May 31, 2025); Nation Fight Elder Fraud Center (NFEFC), https://www.fightelderfraud.org/ (last visited May 31, 2025).; Michelle Singletary, Scam Losses Hit Almost $17 Billion. The Fix Is Bigger than Self-Help., The Washington Post, May 16, 2025, https://css.washingtonpost.com/business/2025/05/16/166-billion-scam-losses-new-record/ (last visited May 31, 2025).

synthetic content can be used to facilitate crimes, such as fraud and extortion."[29] The Washington, DC Attorney General warned "We are witnessing a disturbing upward trend of scammers preying on District residents, particularly seniors, using artificial intelligence to steal their money, sensitive information and data," and the Maryland Attorney General shared last year that "Voices generated by AI are often used in scams. These are fake voices created by computers to sound like real people. Scammers use this technology, mimicking voices and even speech patterns, to trick people into believing they are talking to someone they know or trust. This makes it very difficult to differentiate between a legitimate call and a scam."[30]

The following real-life harms from voice cloning have already occurred, and underline the need for decisive action:

- **Kidnapping Hoax Calls with Cloned Voices:** Scammers use AI voice cloning to simulate a loved one in distress, demanding ransom. In one case, an Arizona mother received a call from what sounded exactly like her daughter crying that "bad men" had her – it was an AI-generated voice mimicry as part of a fake kidnapping scheme.[31] Law enforcement warns that fraudsters leverage *"fake audio or video recordings of people [victims] know, often asking for money to help them get out of an emergency."*[32] Such calls prey on panic, urging immediate payment before the ruse can be uncovered.
- **"Grandparent" or Family-Emergency Impersonation Scams:** Similar voice cloning tactics target relatives, especially seniors.[33] Scammers clone

[29] *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*. (2024, December 3). Federal Bureau of Investigation. https://www.ic3.gov/PSA/2024/PSA241203
[30] *Consumer Alert: Spotting and Avoiding Imposter Scams*. (2024, May 31). Maryland Office of the Attorney General. https://www.marylandattorneygeneral.gov/press/2024/053124CA.pdf
[31] Erielle Reshef, Kidnapping Scam Uses Artificial Intelligence to Clone Teen Girl's Voice, Mother Issues Warning, ABC7 Los Angeles, Apr. 13, 2023, https://abc7.com/ai-voice-generator-artificial-intelligence-kidnapping-scam-detector/13122645/ (last visited May 31, 2025).
[32] *Attorney General Schwalb Issues Consumer Alert to Protect District Residents from Deepfake Telemarketing Scams*. (2025, April 18). Office of the Attorney General for the District of Columbia. https://oag.dc.gov/release/attorney-general-schwalb-issues-consumer-alert-3
[33] Charles Bethea, The Terrifying A.I. Scam That Uses Your Loved One's Voice, The New Yorker, Mar. 7, 2024, https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice (last visited May 31, 2025).

the voice of a grandchild or family member claiming to be in an accident, arrested, or otherwise in urgent trouble. The FTC has cautioned that a caller asking for money urgently, especially via wire or gift cards, is a red flag. In one incident, a victim "*got a call from her daughter's phone and she sent $1,500,*" believing her child needed bail money. Only later did she learn it was an AI-generated impostor. These AI-enhanced "family emergency" scams are on the rise, tricking Americans out of millions.

- **Executive/CEO Voice Impersonation Fraud:** Criminals have cloned company executives' voices to authorize fraudulent transfers. In 2019, scammers mimicked the voice of a German parent company CEO and convinced a U.K. subsidiary to wire them $243,000, believing the instruction was legitimate. More recently, British firm Arup lost approximately $25 million after criminals deep faked the voices (and on video, faces) of its CFO and other colleagues in a virtual meeting, tricking an employee into multiple bank transfers.[34] Such AI-aided "business email compromise" schemes by phone are an alarming evolution of corporate fraud, now reported internationally (e.g., in Europe, Asia) and targeting companies of all sizes.
- **Voice Cloning to Defeat Security Checks:** Beyond person-to-person deception, AI-generated audio impersonates individuals to bypass authentication. The FBI warns that criminals have "obtained access to bank accounts" by using cloned voice clips of the account holder.[35] For instance, if a bank's phone system uses voice-recognition passphrases, a scammer with an AI copy of the victim's voice could fool the system and gain account control. This threat extends to any identity verification that relies on voice, showing how generative AI can subvert security measures and facilitate fraud without needing to "engineer" a human victim socially.

[34] Grace Noto, Scammers Siphon $25M from Engineering Firm Arup via AI Deepfake 'CFO,' CFO Dive, May 17, 2024, https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/ (last visited May 31, 2025).
[35] *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*. (2024, December 3). Federal Bureau of Investigation. https://www.ic3.gov/PSA/2024/PSA241203

B. *There is a whole host of technologies comprising the "scam stack," where the people building and using the technologies should be held responsible.*

Beyond just AI, in a recent publication, CFA highlighted the connection of several pieces of technology we're calling the "scam stack," all of which are fueling an increase in scams. These include:

- Data brokers who sell individuals' data, allowing scams to be hyper-targeted based on behavior, demographics, location, relationships, purchases, and more.
- AI companies that facilitate the faster and easier creation of the content of the messages – text, audio, images, and video.
- Robotexters, robocallers, caller-ID spoofers, underregulated and platforms, videoconferencing software, and mass email platforms that facilitate the delivery of the scam content.
- Payment platforms, banks, crypto wallet providers, and more that facilitate the transfer of funds.
- Methods of reporting – which can be improved on platforms like phone providers, email providers, social media companies, and more, where people often *receive* these.
- There is also the concern about the growing market and advertisement of "AI Agents" – tools that allow a user to have a program "take over" their device to complete a task like grocery shopping or creating documents. While they haven't come to fruition entirely yet, many would require a trustworthy user to screen share and allow remote control.

Adding to the longstanding scourge of scams, the availability of these technologies increases the urgency of swift action.

II. Federal Consumer Protection Agencies Need to Do More to Adequately Protect Consumers

Federal consumer protection agencies tasked with prosecuting and rooting out scam robotexts and robocalls are being stripped down, shut down, and

distracted. The consequence is stark: fewer agency staff hours dedicated to enforcement and rulemakings means more freedom for scammers to operate with impunity, unleashing a torrent of harassing calls and texts that fleece consumers of their hard-earned money and sensitive personal data.

In addition to the primary federal enforcers, the FCC and FTC, which are discussed at length below, attacks on agencies across the government are having ripple effects in preventing improvement in robotexts and robocalls.

In April, the Department of Justice eliminated their Consumer Protection branch entirely.[36] This is the branch that brought a landmark criminal case against a data broker for selling consumer lists of more than 30 million Americans that were used to carry out sweepstakes and other scams against elderly Americans.[37] Throughout 2025, the Consumer Financial Protection Bureau (CFPB) has been the explicit target of the administration. Whether it was multiple attempts at mass firings[38], preventing employees from doing any work[39], closing the physical offices[40], or giving companies that violated the law a corporate pardon[41], the CFPB has been a cop off its beat. When they were allowed to work, CFPB employees offered support to people who have been scammed[42] as a result of

[36] David Dayen, Justice Department Shutting Branch That Prosecutes Consumer Fraud Cases, The American Prospect (2025), https://prospect.org/justice/2025-04-24-justice-department-shuts-branch-that-prosecutes-consumer-fraud-cases/ (last visited May 31, 2025).
[37] Principal Deputy Assistant Attorney General Brian Boynton Delivers Remarks at White House Roundtable on Protecting Americans from Harmful Data Broker Practices, United States Department of Justice (2023), https://www.justice.gov/archives/opa/speech/principal-deputy-assistant-attorney-general-brian-boynton-delivers-remarks-white-house (last visited May 31, 2025).
[38] Stacy Cowley, Mass Layoffs Hit Consumer Financial Protection Bureau, The New York Times (2025), https://www.nytimes.com/2025/04/17/us/politics/consumer-financial-protection-bureau-layoffs.html.
[39] Laurel Wamsley, New CFPB Chief Closes Headquarters, Tells All Staff They Must Not Do "Any Work Tasks," NPR, Feb. 8, 2025, https://www.npr.org/2025/02/08/nx-s1-5290914/russell-vought-cfpb-doge-access-musk (last visited May 31, 2025).
[40] *Id.*
[41] Consumer Federation of America and Student Borrower Protection Center Issue Joint Memorandum on Trump-Led CFPB Pardons of Repeat Offender Corporations · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/consumer-federation-of-america-and-student-borrower-protection-center-issue-joint-memorandum-on-trump-led-cfpb-pardons-of-repeat-offender-corporations/ (last visited May 31, 2025).
[42] Melissa Chan, Democratic Lawmakers Warn Axing Consumer Financial Protection Bureau Will Leave Troops Vulnerable to Fraud and Scams, NBC News, Feb. 20, 2025,

schemes perpetrated over robotexts and robocalls, and continually provide essential support for other enforcement agencies around the country through the maintenance and sharing of the consumer complaint database.[43] The CFPB should also be able to proactively help consumers by intervening with monetary platforms when consumers lose money on platforms like Zelle, Venmo, cryptocurrency wallets, and more.

A. *The FCC's one-track focus on deregulation and censorship is harming consumers. They need both more authorities and a willingness to use them.*

The shadowy, fast-moving, and complicated nature of the robocommunication industry where new businesses pop up, bid on call delivery at scale, and are not adequately incentivized not to deliver illegal calls necessitates bold and robust policies and enforcement from the FCC.[44] As former Commissioner Geoffrey Starks put it in 2021, "As I have long said, illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it. Last year's estimated 46 billion robocalls and last months estimated 4.1 billion calls are proof positive of that. We must therefore continue to be vigilant in our efforts to identify the sources of these calls and stop them in their tracks."[45]

With rising robotexts and robocalls, Americans need an FCC that prioritizes their lived experience of annoyance, frustration, and loss. The FCC was created by Congress to be an agency independent from the President.[46] However, the current

https://www.nbcnews.com/news/us-news/democratic-lawmakers-warn-axing-consumer-financial-protection-bureau-w-rcna192848 (last visited May 31, 2025).

[43] Ahead of CFPB Forum, Banking Committee Releases New Analysis Revealing Precipitous Drop in Consumer Complaints Processed After Trump-Musk Attack on American Consumers, United States Committee on Banking, Housing, and Urban Affairs, https://www.banking.senate.gov/newsroom/minority/ahead-of-cfpb-forum-banking-committee-releases-new-analysis-revealing-precipitous-drop-in-consumer-complaints-processed-after-trump-musk-attack-on-american-consumers (last visited May 31, 2025).

[44] *See e.g.,* Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit* at pp. 25-30, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025);

[45] In re Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks)

[46] The Federal Communications Commission (FCC), National Telecommunications and Information Administration, https://www.ntia.gov/book-page/federal-communications-commission-fcc (last visited May 31, 2025).

FCC Chairman Brendan Carr seems focused on controlling the speech and corporate hiring practices of CBS, NBC, Disney, ABC and more because they are perceived political enemies of the President.[47] FCC Commissioner Anna Gomez described the current actions of the agency as "weaponized to chill speech and to punish the press."[48] Civil society representing viewpoints from all over the political spectrum have expressed concern that this focus is on "grabbing headlines" and takes away from "more important, basic work."[49]

At the same time, Chairman Carr released the "*Delete, Delete, Delete*" initiative, in which Carr asked the American public what regulations from the FCC should be "deleted" because they "stand in the way of deployment, expansion, competition, and technological innovation." The announcement has no mention of consumer protection and runs counter to the dire need for *more* regulation in this space.[50]

In their 2022 report, NCLC and EPIC recommended that the FCC (1) require that all providers in the call path engage in effective mitigation against robocalls, (2) place clear financial consequences on providers who transmit illegal robocalls when they knew or should have known that the calls were illegal, (3) use suspension from the Robocall Mitigation Database as a mechanism to protect telephone subscribers from receiving illegal calls, (4) mandate that tracebacks conducted by the Industry Trace Group are made public, and (5) impose strict

[47] Karl Bode, Brendan Carr's FCC Is an Anti-Consumer, Rights-Trampling Harassment Machine, The Verge, Apr. 28, 2025, https://www.theverge.com/tech/656653/brendan-carr-fcc-anti-consumer-harassment-dei-trump (last visited May 31, 2025).
[48] Liam Reilly, FCC Commissioner Rips a "Weaponized" Agency Punishing News Outlets Trump Dislikes, CNN, May 15, 2025, https://www.cnn.com/2025/05/15/media/fcc-anna-gomez-rips-weaponized-agency-brendan-carr-trump (last visited May 31, 2025).
[49] Liam Reilly, FCC Commissioner Rips a "Weaponized" Agency Punishing News Outlets Trump Dislikes, CNN, May 15, 2025, https://www.cnn.com/2025/05/15/media/fcc-anna-gomez-rips-weaponized-agency-brendan-carr-trump (last visited May 31, 2025).; Brendan Carr's Bizarro World FCC, The Foundation for Individual Rights and Expression, https://www.thefire.org/news/brendan-carrs-bizarro-world-fcc (last visited May 31, 2025); Jessica J. González, How FCC Chairman Carr Has Fueled Trump's Authoritarian Takeover, Free Press (2025), https://www.freepress.net/blog/how-fcc-chairman-carr-has-fueled-trumps-authoritarian-takeover (last visited May 31, 2025).
[50] FCC Opens "In Re: Delete, Delete, Delete" Docket, Federal Communications Commission (2025), https://www.fcc.gov/document/fcc-opens-re-delete-delete-delete-docket (last visited May 31, 2025).

licensing and high bonding requirements for VoIP providers in order to address.[51] These recommendations are still sound and should be adopted by the agency.

Voice and internet service providers should be required to permanently block the worst offenders perpetrating scam calls and online fraud, including upstream providers who facilitate these calls; these bad actors often operate several steps removed from the companies that directly provide services to consumers.[52] The FCC has made progress, but its ability to issue orders against every offender is limited. A better solution would be to require providers to automatically block upstream sources of scam.[53]

The Telephone Consumer Protection Act (TCPA), enacted in 1991, restricts certain types of automated telephone dialing systems as well as the dissemination of artificial or prerecorded voice messages.[54] It's the reason consumers can ask to opt-out of many robocalls, the reason the Do Not Call registry exists, and is *supposed* to require any telemarketer to get "prior express written consent" before making a call. The FCC has strengthened the protections for and tried to limit the amount of robocalls and robo-texts using AI in recent years. However, the current FCC has delayed enforcement for these rules, and they may be the target of the "Delete, Delete, Delete" initiative or other aggressive corporate-friendly deregulation efforts.[55]

---

[51] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit* at pp. 25-30, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025);

[52] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit* at pp. 4-5, 12, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025);

[53] Kayla Ferdinand, Client Advisory on the FCC's Enforcement of the Know Your Customer Rule Against Telnyx, HWG LLP (2025), https://hwglaw.com/2025/02/07/client-advisory-on-the-fccs-enforcement-of-the-know-your-customer-rule-against-telnyx/ (last visited May 31, 2025).

[54] *Robocalls*. EPIC - Electronic Privacy Information Center. https://epic.org/issues/consumer-privacy/robocalls/

[55] FCC Opens "In Re: Delete, Delete, Delete" Docket, Federal Communications Commission (2025), https://www.fcc.gov/document/fcc-opens-re-delete-delete-delete-docket (last visited May 31, 2025); FTC Launches Public Inquiry into Anti-Competitive Regulations, Federal Trade Commission (2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-launches-public-inquiry-anti-competitive-regulations (last visited May 31, 2025).

Last December, the FCC announced that 2,411 voice service providers are at risk of being removed from the Robocall Mitigation Database (RMD) and consequently blocked from the U.S. phone network.[56] Participation in the RMD requires each voice service provider to certify that they are taking certain minimum actions to detect and reduce (or mitigate) the volume of illegal robocall traffic that they transmit through the U.S. phone system; providers are not permitted to accept calls from companies that are not listed in the RMD, so removal from the RMD is tantamount to removal from the U.S. phone network.[57] There need to be better mechanisms to make the RMD useful in protecting consumers, though. There is no requirement, much less an automated mechanism, that non-compliant providers be suspended from the RMD, and the FCC does not have the scale to monitor compliance by each of the 9,856 providers that have registered.[58] The RMD should not simply require a provider to have tools to block bad actors, but a provider at any stage of a call's path should have an affirmative responsibility to block bad actors.[59]

B. The FTC Must Finalize the Individual Impersonation Rule and Prioritize Vigorous Enforcement Against Upstream Actors Facilitating and Supercharging Robotexts and Robocalls

Recent leadership changes at the FTC—most notably the firing of key staff and critically two Democratic commissioners[60]—have left the agency ill-equipped to

---

[56] FCC Opens "In Re: Delete, Delete, Delete" Docket, Federal Communications Commission (2025), https://www.fcc.gov/document/fcc-opens-re-delete-delete-delete-docket (last visited May 31, 2025).
[57] *Id.*
[58] Robocall Mitigation Database Listings, Federal Communications Commission (FCC), https://fccprod.servicenowservices.com/rmd?id=rmd_listings (last visited Jun 1, 2025).; Electronic Privacy Information Center, Public Knowledge, National Consumers League, In Re: Improving the Effectiveness of the Robocall Mitigation Database, EPIC - Electronic Privacy Information Center, https://epic.org/documents/in-re-improving-the-effectiveness-of-the-robocall-mitigation-database/#_ftn20 (last visited Jun 1, 2025).; Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit*, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025).
[59] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit*, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025).
[60] Ashley Gold, Trump Fires Democratic FTC Commissioners, Axios, Mar. 18, 2025, https://www.axios.com/2025/03/18/trump-fires-democratic-ftc-commissioners (last visited May

protect American consumers. It reflects a focus on politics at the expense of consumers. These shifts have drained institutional knowledge, reduced productive internal discussions, and weakened the Commission's ability to respond proactively to emerging threats like robocalls, robotexts, and AI-enabled deception. At a time when bold, strategic enforcement is needed, the FTC risks being less able to act quickly and effectively to protect consumers.

The FTC's 2024 impersonation rules[61] are an important step forward, and CFA is encouraged to see the agency enforcing the government impersonation rule in 2025.[62] While the rule addressing business or government impersonation has been finalized and enforced, the rule addressing impersonation of individuals has not.[63] With the increase availability in voice cloning, it's critical that the FTC finalizes this rule. These technologies make it easier than ever to deceive consumers, often without traditional fraud indicators, and make proactive enforcement more urgent. Since those cloning tools don't have adequate controls against cloning individuals, the FTC must finalize and enforce these rules.[64]

Both rules can give the FTC powerful tools to hold platforms accountable when they allow deceptive impersonation to thrive—especially in cases where developers fail to implement basic safeguards like authentication or content moderation.

31, 2025); Lauren Feiner, FTC Workers Are Getting Terminated, Including Consumer Protection and Antitrust Staff, The Verge, Mar. 3, 2025, https://www.theverge.com/news/623242/federal-trade-commission-terminations (last visited May 31, 2025).

[61] FTC Announces Impersonation Rule Goes into Effect Today, Federal Trade Commission (2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today (last visited May 31, 2025);

[62] FTC Highlights Actions to Protect Consumers from Impersonation Scams, Federal Trade Commission (2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-highlights-actions-protect-consumers-impersonation-scams (last visited May 31, 2025).

[63] FTC to Hold Informal Hearing on Proposed Rule Amendment Banning Impersonation of Individuals, Federal Trade Commission (2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-hold-informal-hearing-proposed-rule-amendment-banning-impersonation-individuals (last visited May 31, 2025).

[64] Grace Gedye, *AI Voice Cloning Report: Do These 6 Companies Do Enough to Prevent Misuse*, Consumer Reports (2025), https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf (last visited May 31, 2025).

The FTC must also avoid a reactive, case-by-case "whack-a-mole" approach as much as possible. It should strategically target the infrastructure enabling these scams. One important enforcement priority is to target the "means and instrumentalities" of crimes like scam texts, such as the agency's *Rytr* case last year.[65] Although that case focused on the use of Generative AI to create endless fake reviews, the same is being done for scam texts.[66] CFA, EPIC, and the National Consumers League offered support for the use of means and instrumentalities to stem harm rather than playing whack-a-mole, and also pushed for stronger remedies "would require companies outputting content to restrict outputs when prompts are clearly intended to violate the law."[67]

Similarly to the FCC, the agency must prioritize enforcement against upstream actors—such as voice service providers and AI developers—who knowingly facilitate these harmful practices.[68] These intermediaries are critical to how illegal calls and texts scale and are essential to accountability. For example, VoIP providers that knowingly transmit robocalls have been successfully prosecuted, resulting in major reductions in complaint volume. These wins resulted in an over 50% decrease in complaints about that problem between 2021 and 2024.[69] Targeting upstream facilitators works—and should be expanded.

---

[65] *Rytr LLC,* 168 F.T.C. 123 (2024) (Docket No. 232-3052), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-approves-final-order-against-rytr-seller-ai-testimonial-review-service-providing-subscribers

[66] Lana Swartz, Alice E. Marwick, and Kate Larson, ScamGPT: *GenAI and the Automation of Fraud*, Data & Society, https://datasociety.net/library/scam-gpt/ (last visited Jun 1, 2025); Ben Winters, *Scamplified* · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).

[67] Consumer Federation of America, Electronic Privacy Information Center (EPIC), and National Consumers League, Comments *In Re Ryr LLC settlement* (FTC-2024-0041) (Nov. 4, 2024), https://consumerfed.org/wp-content/uploads/2024/11/CFA-EPIC-NCL-Rytr-Comment.pdf

[68] Grace Gedye, *AI Voice Cloning Report: Do These 6 Companies Do Enough to Prevent Misuse*, Consumer Reports (2025), https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf (last visited May 31, 2025).

[69] Reports of Unwanted Telemarketing Calls Down More Than 50 Percent Since 2021, Federal Trade Commission (2024), https://www.ftc.gov/news-events/news/press-releases/2024/11/reports-unwanted-telemarketing-calls-down-more-50-percent-2021 (last visited May 31, 2025).; https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-sues-stop-voip-service-provider-assisted-facilitated-telemarketers-sending-hundreds-millions; https://www.ftc.gov/news-events/news/press-releases/2022/04/ftc-takes-action-stop-voice-over-internet-provider-facilitating-illegal-telemarketing-robocalls; https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us

The FTC needs to use the full range of authorities, including the impersonation rules and unfairness doctrine, to disrupt these harmful ecosystems.

III. Congress can and should be doing more to address robocalls and robotexts.

Meaningful consequences and incentives for actors throughout the call path to block illegal calls before they're sent to consumers and root out the entities delivering them should be Congress' priority when addressing robocall and robotexts. Providers transmitting the calls must be held responsible, full stop.

While Congress gave the FCC some tools in the TRACED Act to protect consumers against robocalls, it doesn't go far enough. Enforcement needs to be rigorous, and massive unaddressed gaps remain.[70] Congress should provide a private right of action for key violations of the TRACED Act. For example, the TRACED Act already prohibits VoIP service providers from charging consumers for call blocking technologies, but there are insufficient tools to enforce it. [71] A private right of action would allow consumers to address the scourge of calls that impact them directly. In addition to there being no private right of action for that provision, onerous arbitration clauses that would prevent meaningful action from aggrieved individuals shouldn't be allowed.

We would be honored to work with your staffs to ensure that all legislation, including the Do Not Disturb Act package,[72] reflects this needed focus on enforcement to make a meaningful dent in robocalls and robotexts if reintroduced. Key updates to provisions in the bill would be essential in meaningfully addressing the problem.

---

[70] TRACED Act Implementation, Federal Communications Commission, https://www.fcc.gov/TRACEDAct (last visited May 31, 2025).
[71] *Id* at Section 10.B.
[72] Congressman Frank Pallone, Jr, *Pallone Introduces Comprehensive Legislation to Curb Onslaught of Annoying and Abusive Robocalls* (Jan. 29, 2024), https://pallone.house.gov/media/press-releases/pallone-introduces-comprehensive-legislation-curb-onslaught-annoying-and

Congress can also work to codify principles put forward in a voluntary agreement between all 51 U.S. Attorneys General and major Voice Service Providers in 2019. It included statements for those Voice Service Providers to analyze and monitor network traffic, investigate suspicious calls and calling patterns, and actually shut down that party's ability to originate, route, and terminate calls on its network when found to be violating the law.[73] While that document does explain that "failure to adhere to these principles is not in itself a basis for liability," it doesn't preclude Congress or the FCC from codifying the principles.[74] As is often the case with voluntary agreements between companies and governments, they mean nothing without enforcement. Clearly, this agreement hasn't been implemented vigorously enough.

While not solely focusing on stopping robocalls, CFA also urges the following digital policy pursuits that would address harms caused by robocalls and robotexts and improve the consumer experience in the digital age:

- ***Increase Funding and Resources for State Enforcement Entities*:** Policymakers should allocate more funding and dedicated resources to state Attorneys General offices to enhance their ability to investigate, prosecute, and enforce against robocalls, robotexts, and AI-enabled scams. Many scams target vulnerable populations at the state and local level, and state AGs are often best positioned to assist victims and hold perpetrators accountable. With the resources they have, all 51 attorneys general have made significant efforts through their Anti-Robocall Litigation Task Force.[75] Additional staff, specialized training, and advanced investigative tools can empower state enforcers to more proactively monitor for AI-powered fraud, take swift action, and deliver meaningful penalties. This two-pronged approach - benefiting victims through restitution and

[73] 51 Attorneys General and Telecom Companies, State AGs Providers AntiRobocall Principles-With Signatories, (Aug. 28, 2019), https://oag.ca.gov/system/files/attachments/press-docs/State%20AGs%20Providers%20AntiRobocall%20Principles-With%20Signatories.pdf (last visited Jun 1, 2025).
[74] *Id*.
[75] North Carolina Department of Justice, *Anti-Robocall Litigation Task Force | Warning Notices* (last visited June 1, 2025), available at https://ncdoj.gov/protecting-consumers/telephones-telemarketing/fighting-robocalls/warning-notices/

compensation, while also serving as a strong deterrent against future scams - can be a powerful complement to the other policy recommendations. Equipping state-level consumer protection agencies with the necessary resources is crucial to combating the growing threat of AI-enabled scams in communities across the country.

- ***Pass a law explicitly exempting Generative AI companies from Section 230, or otherwise place legal responsibility for reasonable content moderation.*** Recent discussions around Section 230 of the Communications Decency Act have included attempts to explicitly bar artificial intelligence (AI) companies from its protections, particularly through the bipartisan No Section 230 Immunity for AI Act introduced by Senators Josh Hawley (R-Mo.) and Richard Blumenthal (D-CT). This legislation seeks to amend Section 230 to hold AI companies accountable for the content generated by their algorithms. Advocates for this change argue that AI-generated content can pose unique risks, including the spread of misinformation, harmful deepfakes, and other deceptive practices that may not be adequately addressed under the current framework. The Hawley-Blumenthal bill aims to clarify that AI companies should be liable for the outputs of their systems, especially when those outputs can lead to real-world harm. This legislative effort reflects growing concerns about the ethical implications of AI technologies and the responsibility of developers to ensure that their systems do not contribute to societal issues.
- ***Establish Transparency and Explainability Requirements for All AI Systems:*** Policymakers should mandate that AI companies provide clear and accessible explanations of how their systems work, including the data inputs, algorithms, and potential biases. This should also include moderation details for companies of a certain size. This transparency can help identify vulnerabilities that scammers may exploit and identify the appropriate actors for responsibility.
- ***Establish Mandatory Reporting and Information Sharing Practices****:* Congress should encourage or require all platforms used for creation and distribution of these scams to offer easy, one-click reporting to the appropriate authorities from the platform that they experienced the scam

on. This reduces a barrier to reporting and puts that additional work on the entity better positioned to do so.

- ***Pass Comprehensive Privacy Law; Mandate real data minimization in privacy laws***. Data minimization is the concept that data can only be collected and used for a specific purpose requested or expected by a consumer. This is often referred to as a ban on secondary data uses, including sales. The development of new technologies like Generative AI systems shouldn't be able to be built on people's work, output, and life without actual informed consent.
- ***Empower people to sue for harms they face in a privacy or AI law.*** A private right of action empowers individuals harmed by violations of privacy or AI laws to sue violators. While enforcement agencies are often well poised to address these harms, the incentives are off when harms are not widely knowable.

CFA vehemently opposes the state AI regulation moratorium[76] provision in the reconciliation bill that passed the house.[77] The scale of these problems is one of many reasons it's not the time to restrict states from regulating the ways AI is causing harm. If states can create transparency or establish appropriate liability regimes for some of the tools in the scam stack, we should welcome it, embracing the critical roles of states not only to protect consumers but be the laboratory of democracy.[78]

IV. Conclusion

Robocalls and robotexts are not just an inconvenience—they are a growing vector for financial fraud, emotional distress, and personal data theft. These harms are

[76] Julia Edinger, State AI Regulation Ban Clears U.S. House of Representatives, GovTech, May 23, 2025, https://www.govtech.com/artificial-intelligence/state-ai-regulation-ban-clears-u-s-house-of-representatives (last visited May 31, 2025).
[77] CFA Statement on dangerous Attempt by the House to Quash All State AI Regulation, Consumer Federation of America (May 12, 2025), available at https://consumerfed.org/press_release/cfa-statement-on-dangerous-attempt-by-the-house-to-quash-all-state-ai-regulation/
[78] Kara Williams & Ben Winters, Debunking Myths About AI Laws and the Proposed Moratorium on State AI Regulation, Tech Policy Press, May 28, 2025, https://www.techpolicy.press/debunking-myths-about-ai-laws-and-the-proposed-moratorium-on-state-ai-regulation/ (last visited May 31, 2025).

increasingly supercharged by generative AI and a loosely regulated "scam stack" of technologies and platforms that enable bad actors to target consumers at scale, with disturbing precision and plausibility. As this threat escalates, our current regulatory framework is not only insufficient—it is actively being dismantled.

Congress must act. Federal consumer protection agencies need not only stronger tools and authorities but also the political and institutional will to use them. Agencies like the FTC, FCC, and CFPB must be empowered, resourced, and restored to aggressively protect consumers—especially the most vulnerable. We must also confront the technologies enabling these scams at every level, from voice-cloning tools and data brokers to voice service providers and payment platforms.

Inadequate action from the FTC and FCC as well as Congress gives a green light to scammers. Congress has the power to lead a coordinated, comprehensive response—one that prioritizes prevention, accountability, and consumer safety. The American people deserve nothing less.

Thank you again for the opportunity to testify. CFA is eager to answer any questions and help you help consumers.

/s/ Ben Winters
Director of AI and Privacy
Consumer Federation of America
bwinters@consumerfed.org