

[Updates](#)

September 03, 2024 (UPDATED October 10, 2024)

FCC Fines Telecom That Transmitted AI-Generated Deepfake Robocalls Impersonating President Biden



Two days before the 2024 New Hampshire Democratic primary, thousands of voters received robocalls, purportedly in the voice of President Joe Biden, telling them not to vote in the upcoming election.

The prerecorded messages falsely implied that voters would not be able to participate in the general election if they cast a vote in the primary. The recordings urged recipients to “save [their] vote for the November election.”

The president’s voice was fabricated using artificial intelligence (AI) technology, and the calls were placed using falsified—or “spoofed”—caller ID information. The phone number that appeared on recipients’ caller IDs was that of a local political operative who was not involved. Despite these efforts at concealment, a political consultant was later indicted for orchestrating the AI-generated deepfake calls. The consultant faces felony charges of voter suppression, along with a proposed \$6 million fine by the Federal Communications Commission (FCC) for purportedly violating the Truth in Caller ID Act by transmitting illegal robocalls using misleading and inaccurate caller ID information with the intent to defraud and cause harm to consumers.

FCC Settlement With Telecom Vendor

Lingo Telecom (Lingo), the voice service provider that transmitted the spoofed calls, has now agreed to pay the FCC \$1 million and implement a rigorous compliance program to settle its role in the disinformation campaign. The [settlement](#) addresses Lingo’s alleged failure to adhere to the FCC’s “[STIR/SHAKEN](#)” caller ID authentication rules, which require that voice service providers use public key cryptography and digital certificates to authenticate their customers’ caller ID information, ensuring that accurate caller ID information is displayed to call recipients.

Life Corporation, a longtime customer of Lingo, transmitted the spoofed calls to Lingo. Lingo then authenticated the spoofed call traffic by providing it with an A-level attestation before originating the calls onto the public switched telephone network (PSTN). This meant that Lingo (1) was responsible for the origination of the calls,

(2) had a direct authenticated relationship with the caller and could identify the caller, and (3) had established a verified association with the number used for the calls. But in this case, Lingo had erroneously concluded that Life Corporation could use the telephone number that appeared to call recipients based on (1) Life Corporation's assurances that it would identify its customers and had verified the telephone numbers of its customers, (2) prior "Know-Your-Customer" (KYC) research Lingo had conducted on Life Corporation, and (3) its 16-year history with Life Corporation. It did not otherwise independently ascertain the legitimacy of the calls or that Life Corporation was authorized to use the displayed number.

The settlement offers no indication that Lingo was aware of the nature of the calls. Nonetheless, the FCC determined that the implementation of reasonable KYC protocols could have mitigated the political consultant's scheme and assessed a historic penalty on Lingo for its alleged failure to properly authenticate its customers.

Takeaways

The 2024 election is the first to feature the widespread use of deepfaked robocalls generated by AI. The Biden deepfake, specifically targeted to suppress voter turnout, highlights the danger of the use of AI to mislead voters.

Though several states have promulgated laws governing AI and deepfakes in political advertising, there are currently no federal rules directly addressing the use of AI-generated content in political communications. The Federal Election Commission, the federal agency overseeing federal campaigns, has signaled that it will not address AI specifically, with at least three of its six commissioners poised to [reject a proposed rulemaking](#) on the use of AI. The FCC recently proposed [rules](#) to require disclosure of the use of AI in political communications, but those rules likely will not be finalized before the 2024 election.

As regulators grapple with the emergence of AI, civil agencies and prosecutors still have other tools to combat political disinformation, including laws governing wire fraud, "paid for by" disclaimers, and voter suppression. The STIR/SHAKEN framework has proven to be another tool, unknown to many in the political community, that can be used to address fraudulent political activity, even where a vendor unknowingly participates in that activity. Those involved in political communications at any stage of an ad's production or distribution would be well served to implement thorough compliance procedures to ensure authentication of their customers.

We recommend consulting with counsel to adopt a robust compliance program built to address the ever-changing regulatory scheme surrounding political communications. Vendors should consult with counsel to review political ads when needed in advance of their distribution, advise on proper use of caller ID information and adherence to FCC political calling rules, and ensure that contracts with clients engaged in political communications include proper indemnification clauses. In addition, we are closely tracking related regulatory developments, including the FCC's [pending rulemaking](#) that proposes to require the disclosure of AI-generated content in political ads. The Communications industry group and Political Law practice at Perkins Coie work together to help vendors and political clients implement the proper safeguards to ensure regulatory compliance.

Update:

On September 26, 2024, the FCC [adopted a \\$6 million forfeiture order](#) against the apparent mastermind of the voter suppression operation, Steve Kramer, a political consultant, for violations of the Truth in Caller ID Act. Kramer admitted to concocting the robocall scheme without the knowledge of his client, Congressman Dean Phillips, who ran for the Democratic nomination against President Joe Biden. The New Hampshire attorney general indicted Kramer for the same scheme earlier this year.

The FCC has long maintained a “totality of the facts and circumstances” test to determine the party responsible for making an unlawful robocall. Such a party must be “so involved in placing the call as to be deemed to have initiated it.” Kramer admitted to drafting the robocall script, hiring an acquaintance to create the AI voice-cloned (or “deepfake”) messages in the voice and tone of President Biden, selecting the telephone number of a prominent New Hampshire political operative unaffiliated with the scheme, and directing a third-party company to transmit the calls to Lingo. For these reasons, the FCC determined that even though Kramer did not physically place the spoofed calls, he initiated them, nonetheless.

This marks the third FCC enforcement action against political robocall campaigns since the last presidential election, joining a [\\$10 million fine](#) levied against Kenneth Moser in 2020 and a [\\$5 million fine](#) levied against John Burkman and Alexander Wohl in 2023. The FCC also renewed and updated its [political robocall and robotext consumer guide](#) in July of this year in anticipation of election season.

The Kramer decision represents the first enforcement action involving deepfake message content since the FCC [proposed new rules](#) for AI-generated robocalls this past August. The rules would require, among other things, that callers obtain consent from called parties prior to placing robocalls or robotexts with AI-generated content.

Authors

Explore more in

[Technology Transactions & Privacy Law](#) [Political Law](#) [Corporate Political Activity](#) [Communications](#)
[Artificial Intelligence & Machine Learning](#)

Related insights

Update

[FTC Proposes Rule Addressing Use of AI To Impersonate Individuals](#)

Update

[FCC Declares AI-Generated Robocalls Unlawful](#)