A Changing Landscape: Novel Cases in Robocall Enforcement

Jessica Kinsey
Attorney-Advisor,
Enforcement Bureau
Federal Communications Commission

Disclosure

Anything written or said in this presentation are my own views and do not represent the views or opinions of the Federal Communications Commission, the Chairwoman, or any of its Commissioners.

FCC Enforcement Bureau
Telecommunications Consumers Division
Robocall Response Team

- The Bureau is responsible for enforcing the provisions of the Communications Act, as amended, the Commission's rules, orders, and various licensing terms and conditions.
- Team robocall falls under the Telecommunications Consumers Division.
- Protecting consumers from unwanted calls, including illegal and spoofed robocalls, is a top priority.
- Common rule violations relate the following:
  - Telephone Consumer Protection Act – prohibits making certain pre-recorded calls without consent;
  - Truth In Caller ID Act – prohibits malicious spoofing;
  - Know-Your-Customer (64.1200(n)(4)) and Know-Your-Upstream-Provider (64.1200(n)(5)) requirements; and
  - STIR/SHAKEN and robocall mitigation plan requirements.

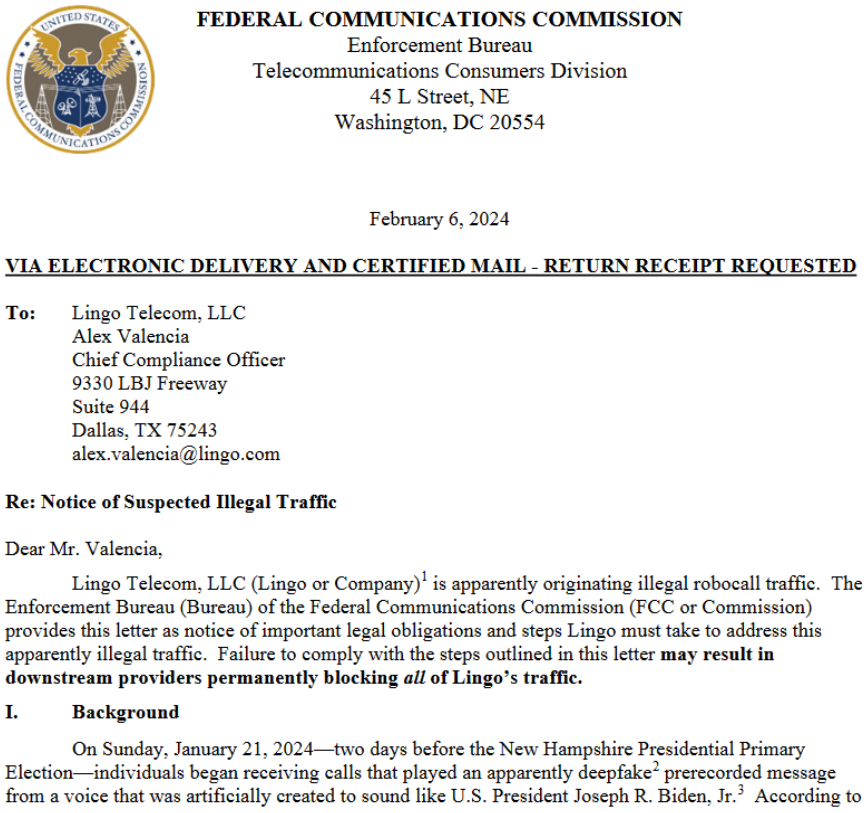
Two-Step Enforcement Strategy

Step 1: Disrupt Calls by Call Blocking

- Prompt action to stop extremely harmful calls
- Cease and desist letter warning service provider
- Public Notice to warn industry and public about potential bad actor

Step 2: Hold Responsible Party Accountable

- Issue citations
- Notice of Apparent Liability
- Consent Decree
- Forfeiture Order
- Collaborate with domestic and foreign counterparts



FEDERAL COMMUNICATIONS COMMISSION
Enforcement Bureau
Telecommunications Consumers Division
45 L Street, NE
Washington, DC 20554

February 6, 2024

VIA ELECTRONIC DELIVERY AND CERTIFIED MAIL - RETURN RECEIPT REQUESTED

To: Lingo Telecom, LLC
Alex Valencia
Chief Compliance Officer
9330 LBJ Freeway
Suite 944
Dallas, TX 75243
alex.valencia@lingo.com

Re: Notice of Suspected Illegal Traffic

Dear Mr. Valencia,

Lingo Telecom, LLC (Lingo or Company)[1] is apparently originating illegal robocall traffic. The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) provides this letter as notice of important legal obligations and steps Lingo must take to address this apparently illegal traffic. Failure to comply with the steps outlined in this letter **may result in downstream providers permanently blocking *all* of Lingo's traffic.**

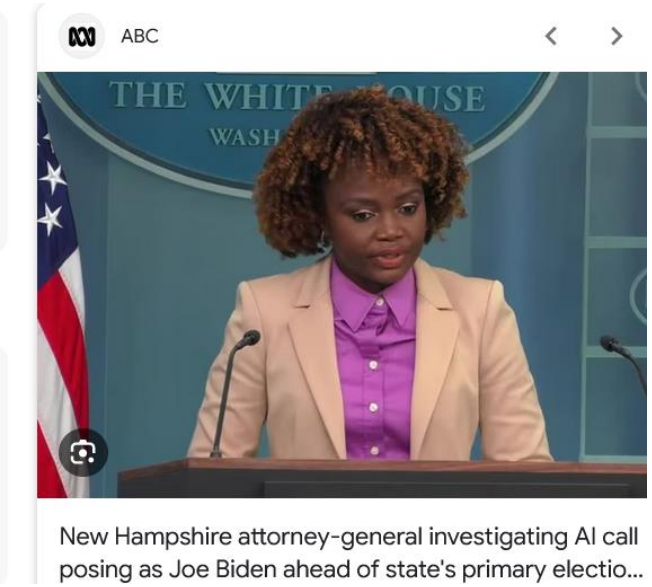
I. Background

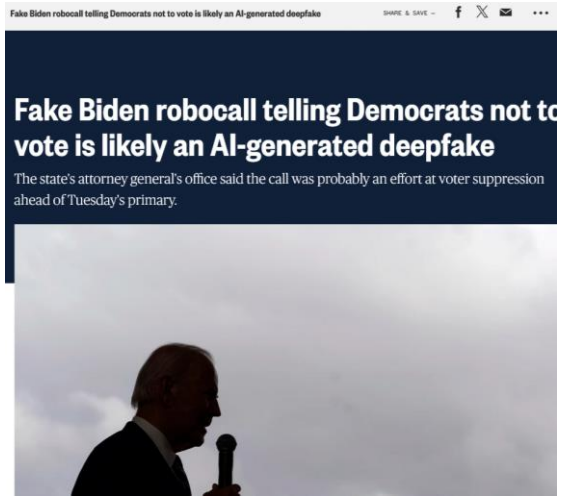
On Sunday, January 21, 2024—two days before the New Hampshire Presidential Primary Election—individuals began receiving calls that played an apparently deepfake[2] prerecorded message from a voice that was artificially created to sound like U.S. President Joseph R. Biden, Jr.[3] According to

Discussion Overview

- Cases are not always straightforward.
- As robocallers become more sophisticated, and as new technologies, such as AI generative calls, develop, we must use new and existing tools to meet those enforcement challenges.
- Two recent cases illustrate how we address novel issues.
  - Case #1 (Lingo Telecom LLC ("Lingo")): Addressed a provider's non-compliance with STIR/SHAKEN rules as it generated spoofed AI-generated political calls meant to influence NH primary.
  - Case #2 (Prince Anand and PZ/Illum): Led to a new way to label and target recidivist threat actors domestically and internationally.

Case #1: Breaking News:
AI Robocalls Disrupt NH Presidential Primary





This coming Tuesday is the New Hampshire Presidential Preference Primary . . . . We know the value of voting Democratic when our votes count. It's important that you save your vote for the November election . . . . Your vote makes a difference in November, not this Tuesday. . .

Investigative Findings

- Caller ID displayed the number of a New Hampshire Political Operative.
- Tracebacks confirmed spoofed caller ID.
- Tracebacks showed false STIR/SHAKEN attestation.
- Tracebacks showed the following call path:
  - Lingo Telecom (originating voice service provider)
  - Life Corporation (call generator/dialing platform)
  - Steve Kramer (client)
- AI technology from ElevenLabs used for deepfake message.

Investigative Findings (continued)

Robocaller: Steve Kramer, CEO, Get Out The Vote

- Steve Kramer is CEO of Get Out The Vote ("GOTV").
- Kramer hired Paul Carpenter to create the message.
- Carpenter is a self-described Magician, hypnotist, and escape artist and expert on all things "AI".
- Carpenter used generative AI voice technology from ElevenLabs to make the messages.

Content creator: Paul Carpenter, "Expert on all things AI"

False Authentication of Spoofed Calls

- Lingo was the originating provider for the calls.
- Lingo signed Life's spoofed traffic with an incorrect attestation without having established that Life had a verified association with the telephone numbers used.
- ATIS-1000074 provided several examples of ways to establish a verified association with the phone number.
- Lingo did not have an evidentiary basis to apply an A attestation.
- Lingo's incorrect attestation showed glaringly deficient KYC practices.
- First case involving violation of 64.6301.

5.2.4 Attestation Indicator ("attest")

The "attest" claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

The SHAKEN framework defines the following three levels of attestation:

A. **Full Attestation:** The signing service provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing service provider is asserting that their customer can "legitimately" use the TN that appears as the calling party (i.e., the Caller ID). The legitimacy of the TN(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The TN was assigned to this customer by the signing service provider.
- This TN is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a TN (e.g., by business agreement or evidence the customer has access to use the number). This includes TNs assigned by another service provider.
- The TN is not permanently assigned to an individual customer, but the signing provider can track the use of the TN by a customer for certain calls or during a certain timeframe.

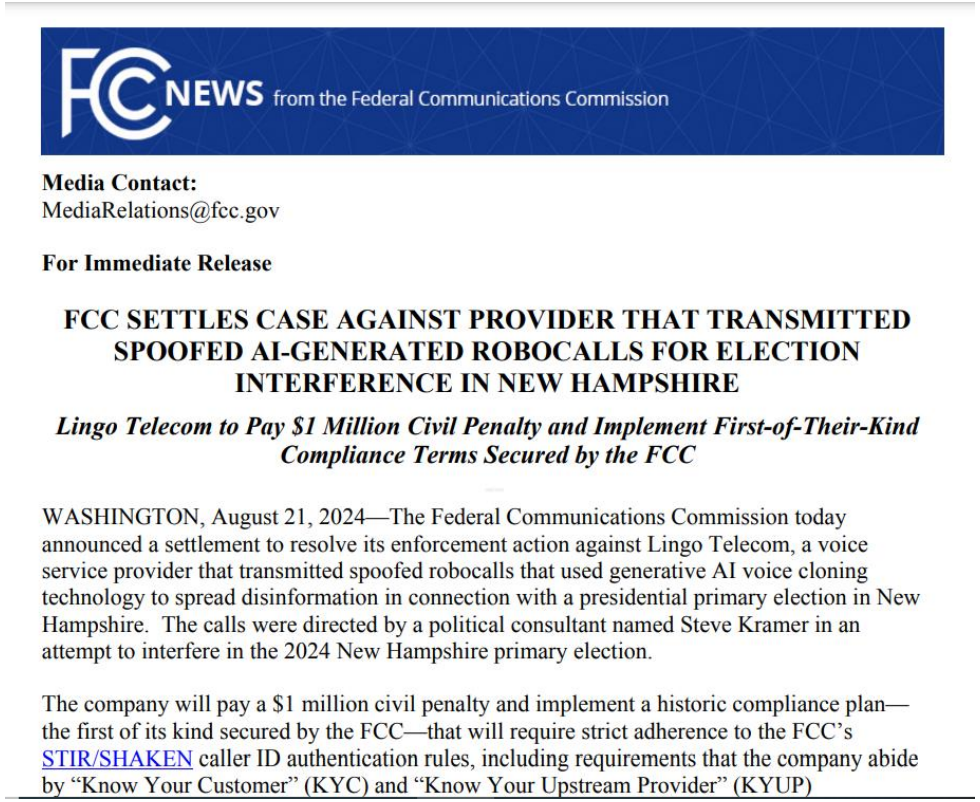
NOTE 2: Ultimately it is up to service provider policy to decide what constitutes "legitimate right to assert a TN" but the service provider's reputation may be directly dependent on how rigorous they have been in making this assertion.

Role of KYC Practices in the STIR/SHAKEN Framework

- KYC Procedures (47 CFR § 64.1200(n)(4)): providers must take affirmative, effective measures to prevent customers from originating illegal calls.
- KYUP Procedures (47 CFR § 64.1200(n)(5)): providers must take reasonable and effective steps to ensure that any provider, foreign or domestic, from which it directly receives traffic is not carrying or processing a high volume of illegal traffic.
  - We do not prescribe specific standards, but the procedures must but effective.
- A provider's KYC practices can determine the amount of evidence available to substantiate an attestation level.
- Deficient procedures which result in incorrect A, or even B, attestation degrade confidence in STIR/SHAKEN authentication.
- Incorrect attestation can increase the likelihood that spoofed calls will bypass a terminating providers' network analytics designed to block spam calls.

Lingo's Consent Decree

- On August 21, 2024, Lingo entered into a consent decree.
- The consent decree contained the following terms:
  - A civil penalty of $1,000,000.
  - Requirement to implement a robust compliance plan including the following:
    - Apply an A-level attestation to calls only if Lingo Telecom itself has provided the originating phone number.
    - Develop enhanced KYC and Know-Your-Upstream provider standards with supporting records.
    - Shall not accept payment in the form of cryptocurrency, gift cards, or cash to transmit or originate calls.



FCC NEWS from the Federal Communications Commission

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC SETTLES CASE AGAINST PROVIDER THAT TRANSMITTED SPOOFED AI-GENERATED ROBOCALLS FOR ELECTION INTERFERENCE IN NEW HAMPSHIRE

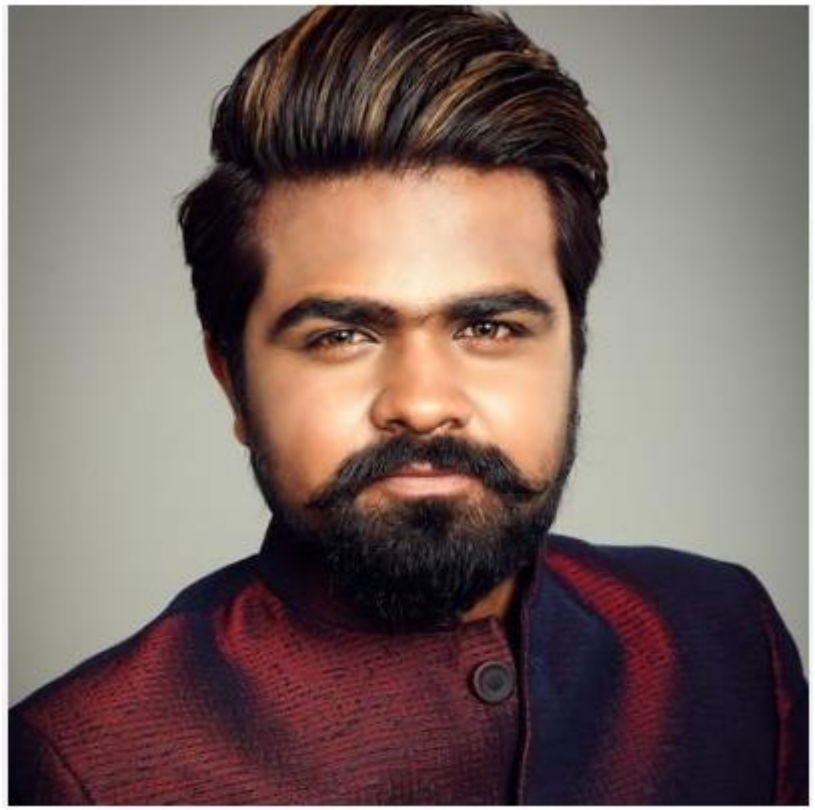
Lingo Telecom to Pay $1 Million Civil Penalty and Implement First-of-Their-Kind Compliance Terms Secured by the FCC

WASHINGTON, August 21, 2024—The Federal Communications Commission today announced a settlement to resolve its enforcement action against Lingo Telecom, a voice service provider that transmitted spoofed robocalls that used generative AI voice cloning technology to spread disinformation in connection with a presidential primary election in New Hampshire. The calls were directed by a political consultant named Steve Kramer in an attempt to interfere in the 2024 New Hampshire primary election.

The company will pay a $1 million civil penalty and implement a historic compliance plan—the first of its kind secured by the FCC—that will require strict adherence to the FCC's STIR/SHAKEN caller ID authentication rules, including requirements that the company abide by "Know Your Customer" (KYC) and "Know Your Upstream Provider" (KYUP)

Case #2: Prince Anand and PZ/Illum

- PZ Telecommunications and Illum Telecommunications (PZ/Illum) were U.S.-based companies that transmitted government imposter, credit card interest rate, and utility calls between August and October 2021.
- Issued cease and desist letter (CDL) to PZ/Illum in October 2021.
- PZ/Illum's CEO started One Eye in October 2021.
- Started call blocking process against One Eye in February 2023.
- Presence of related entities in India, UAE, and UK necessitated a strategy for multinational robocalling operations.



Prince Anand, PZ/Illum CEO

New Enforcement Tool: C-CIST

- Consumer Communications Information Services Threat (C-CIST) is a new designation for the worst of the worst robocallers.

- Applies to threat actors that continuously meet the following criteria:
  1. Use U.S. networks to perpetuate harmful schemes; and
  2. Evade liability for their actions.

- Helps enforcement efforts in three ways:
  1. Heightens awareness of particularly nefarious actors;
  2. Provides our international partners with another way to identify known threats before they reach U.S. networks; and
  3. Provides industry stakeholders with information to fortify their "Know Your Customer" and "Know Your Upstream Provider" processes.

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC ENFORCEMENT BUREAU ISSUES FIRST OF ITS KIND CONSUMER COMMUNICATIONS INFORMATION SERVICES THREAT (C-CIST) CLASSIFICATION FOR REPEAT ROBOCALL BAD ACTOR

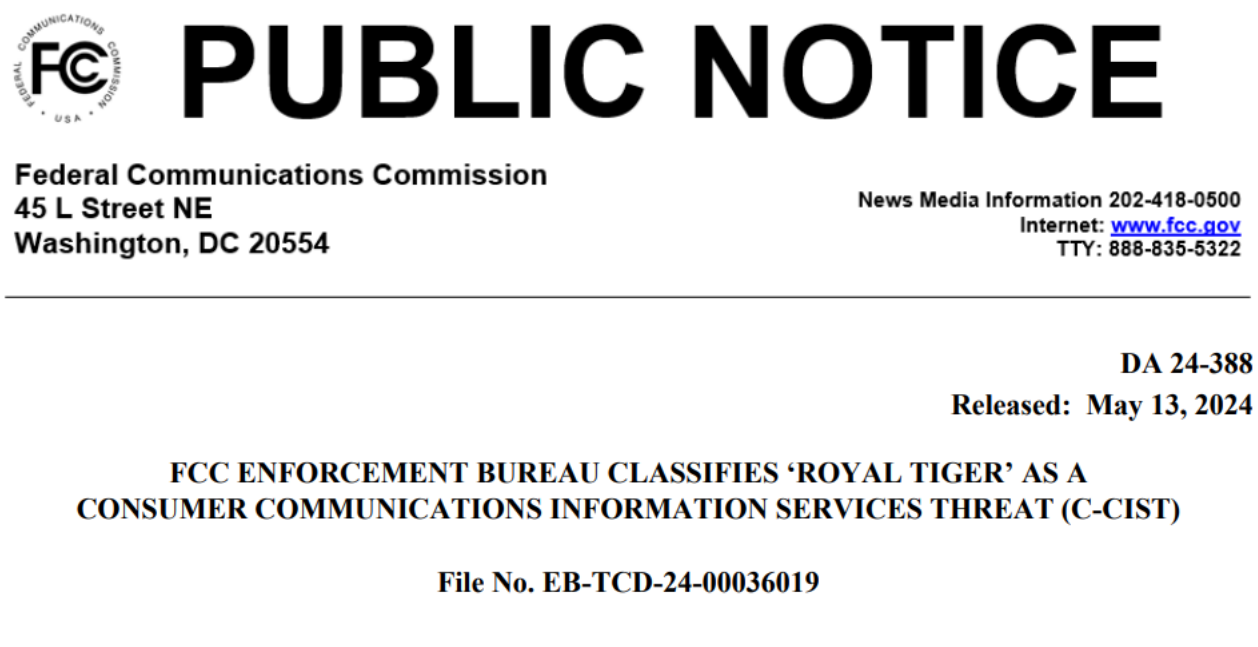
C-CIST Classification for 'Royal Tiger' Group Will Assist International Regulatory Counterparts and Law Enforcement Partners with Tracking Bad Actors and Help Industry Better Utilize 'Know Your Customer' Protocols

WASHINGTON, May 13, 2024—The FCC's Enforcement Bureau today, for the first time, officially classified a group of entities and individuals persistently facilitating robocall campaigns, aimed at defrauding and harming consumers, as a Consumer Communications Information Services Threat (C-CIST) to empower its international anti-robocall fighting partners with another way to identify known threats before they reach U.S. networks. Building upon its recent "Spring Cleaning" initiative and enforcement actions combatting calls that facilitated the misuse of generative artificial intelligence (AI) voice-cloning technology, the C-CIST classification will be an additional tool that allows the Bureau to formally name threat actors that are repeatedly using U.S. communications networks to perpetuate the most harmful, illegal schemes against consumers. These perpetrators commonly attempt to use multiple companies, opaque and convoluted corporate structures, shifting addresses, and other tactics, techniques, and procedures to evade consequences for illegal activities and continue profiting at the expense of consumers. The C-CIST classification will also provide industry stakeholders with information to enhance their "Know Your Customer" and "Know Your Upstream Provider" processes.

In a Public Notice released today, the Bureau classified a group of individuals and entities it is identifying as "Royal Tiger" as the first designated C-CIST. Royal Tiger and its associates operate in India, the United Kingdom, the United Arab Emirates, and the United States. The

Royal Tiger: The First C-CIST

- On May 13, 2024, Prince Anand, Kaushal Bhavsar, PZ/Illum, and One Eye, which we named Royal Tiger became the first C-CIST.
- Designated a C-CIST because of Royal Tiger's harm to consumers, recidivism, and history of enforcement actions with other agencies.
- C-CIST label allows for easier identification of the threat these actors pose.
- As our investigative targets use more sophisticated techniques, the C-CIST classification will be a useful tool to distinguish the most harmful threat actors.



PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov
TTY: 888-835-5322

DA 24-388
Released: May 13, 2024

FCC ENFORCEMENT BUREAU CLASSIFIES 'ROYAL TIGER' AS A CONSUMER COMMUNICATIONS INFORMATION SERVICES THREAT (C-CIST)

File No. EB-TCD-24-00036019

By the Chief, Enforcement Bureau:

The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) issues this Public Notice to notify domestic and international law enforcement partners, industry stakeholders, and consumers that it has classified a group of individuals and entities, which it identifies as "**Royal Tiger**," as a Consumer Communications Information Services Threat (C-CIST). **Royal Tiger** has a presence in India, the United Kingdom, the United Arab Emirates, and the United States.

Questions?