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

FACT SHEET

Consumer Communications Information Services Threat (C-CIST) Designation

Threat actors in the communications space are able to decentralize operations across multiple jurisdictions by using shell companies, deceitful corporate structures, changes of address, and similarly deceptive tactics in order to evade detection and enforcement. More frequently, they are victimizing consumers using information harvested from data breaches and cyber intrusions, utilizing "spoofing" technology to falsely appear to be calling from a trusted phone number, and deploying generative artificial intelligence (AI) voice-cloning technologies to further target victims. Ensuing fraudulent and unlawful calls to consumers can result in significant financial loss and disruptive intrusions that erode trust in critical consumer communications infrastructure.

The Federal Communications Commission's Enforcement Bureau is adopting the Consumer Communications Information Services Threat (C-CIST) classification to shine a light on the tactics, techniques, and procedures of a C-CIST's illegal operation. This will allow state, federal, and international regulatory counterparts and law enforcement entities to quickly detect and pursue appropriate action against these threat actors. The classification will also arm industry stakeholders with information that will enhance their "Know Your Customer (KYC)" and "Know Your Upstream Provider (KYUP)" processes. Industry stakeholders are the first line of defense in keeping illegal and harmful traffic off U.S. communications networks.

The C-CIST classification advances a "whole-of-government" and "public/private sector" approach to protecting consumers and businesses from harmful threat actors.

Frequently Asked Questions

Why does the Enforcement Bureau consider these types of actors a special kind of threat?

C-CISTs have repeatedly violated (or apparently violated) robocalling rules and have been the subject of one or more FCC enforcement actions. They may seek to evade accountability and further their illicit conduct by hiding behind a charade of shell companies. Moreover, the most egregious threat actors in this space target people through illegal robocalls and scam text messages using information harvested from data breaches and cyber intrusions.

Why is the Enforcement Bureau giving this kind of threat a specific name?

We want to marshal all of our resources to address the consumer harm and privacy risks C-CIST actors unleash on the public by utilizing a term that provides government and industry stakeholders with a common focus and the ability to identify and address these actors for attribution and enforcement purposes across state, federal, and international jurisdictions.

How did the Enforcement Bureau develop this tool?

The Enforcement Bureau is responsible, through delegated authority, for enforcing the provisions of the Communications Act of 1934, as amended, and the Commission's rules. Our mission is also to protect consumers from bad actors who seek to misuse communications information services to inflict harm upon

the public through malicious and illegal calling and texting campaigns designed to defraud and instill fear. The C-CIST strategy is similar to how the Advanced Persistent Threat (APT) labeling approach is used to identify and track sophisticated cybercriminals and foreign adversary state actors for notice, tradecraft, and attribution purposes.

What is the criteria to be considered a C-CIST?

The Enforcement Bureau classifies a party as a C-CIST whose misconduct—in either nature or scope—poses a significant threat to consumer communication information services. We reserve this label for especially troubling actors who have been involved in defrauding or harming consumers and businesses in a way that we see as presenting an ongoing risk worthy of special attention.

Will you be creating something like a "covered list" or a database for this classification?

We publicize our enforcement actions on the Enforcement Bureau's website, including whether we have classified a party as a C-CIST.

Will these classifications, and the threats that the C-CISTs are known for, be publicized? And if so, how?

We publicize our enforcement actions on the Enforcement Bureau's website, and typically describe the nature of the threat.

What will the consequences be for those who are named as a C-CIST?

First and foremost, these actors thrive by operating in the shadows. This classification shines a very bright light on them for law enforcement, industry stakeholders, consumers, and businesses. Second, the FCC will use the full extent of its authority to prevent these actors from accessing the U.S. telecommunications space in a way that harms consumers. These enforcement actions may include cease-and-desist letters, removal from the Robocall Mitigation Database, and forfeiture orders. However, the appropriate action will be tailored to the party and its conduct. For example, in 2023, the Enforcement Bureau ordered immediate downstream providers to block traffic from One Eye LLC. This was the first such action taken against a gateway provider.

Has the Enforcement Bureau coordinated this designation/classification with other regulators or entities? If so, which ones?

The Enforcement Bureau identified the need for this classification and designed this approach. However, as with many important initiatives, we are coordinating with the DOJ, FTC, state Attorneys General offices, international regulators, and numerous industry stakeholders.

Are there certain kinds of schemes you are seeing that are the impetus for this new designation/classification? If so, what are they?

This classification is meant for recidivist robocallers that transmit particularly nefarious traffic that poses a threat to consumers and businesses. Threat actors classified as C-CISTs may have been the subjects of prior enforcement actions for facilitating particularly harmful and apparently unlawful robocall campaigns, may have attempted to evade liability for their actions, and may have operated in or have connections to multiple jurisdictions.