wiley

ALERT

Robocall Enforcement: Voice Providers Should Take Note of FCC's New "C-CIST" Designation for Actors Posing a "Significant Threat" to Communications Services

May 16, 2024

On May 13, the Federal Communications Commission's (FCC or Commission) Enforcement Bureau (Bureau) classified for the first time a group of entities and individuals – dubbed "Royal Tiger" – as a Consumer Communications Information Services Threat (C-CIST). This first-of-its-kind FCC designation represents a new development on the robocall front that all voice providers should closely monitor. In an accompanying Public Notice, the Bureau defines a C-CIST as a party whose "misconduct – either in nature or scope – poses a significant threat to consumers' trust in, and ability to use, communications information services." The Bureau also issued a Press Release, Enforcement Advisory, and Fact Sheet addressing this new classification.

The Bureau's Basis for the C-CIST Designation

The Bureau states that it is creating and applying this label for the first time "to heighten awareness of these threat actors among our law enforcement partners and industry stakeholders" and to "ensure that these threat actors are readily detected and blocked from perpetuating potentially unlawful schemes that compromise our communications information services and harm consumers." Moreover, the Bureau's fact sheet classified C-CISTs as individuals and entities who "have repeatedly violated (or apparently violated)" the Commission's rules and have been the subject of one or more FCC enforcement actions. Below we provide: (1) an overview of the Bureau's first C-CIST classification; (2) additional information on the

Authors

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Kelly Laughlin
Associate
202.719.4666
klaughlin@wiley.law

Practice Areas

Telecom, Media & Technology
Telecommunications & Broadband Service
The Telephone Consumer Protection Act (TCPA)

new classification system; and (3) recommendations for industry.

The Royal Tiger Entities and Individuals Are No Strangers to Robocall Enforcement

According to the Public Notice, Royal Tiger is led by Prince Jashvantlal Anand and his associate Kaushal Bhavsar. The Public Notice also explains that through Anand and Bhavsar, Royal Tiger has operated three originating or gateway providers – Illum Telecommunication Limited, PZ Telecommunication LLC, and One Eye LLC – to make calls to U.S. consumers. Notably, the FCC issued its first-ever Robocall Blocking Order against One Eye LLC in May 2023, and a Cease and Desist Letter to PZ/Illum in October 2021.

The Public Notice also states that the individuals own and operate multiple Indian and United Kingdom companies that are used to make calls in the United States. And according to the Public Notice, "Royal Tiger has facilitated imposter scams, including calls that spoofed phone numbers for financial institutions such as banks." Moreover, many of the calls facilitated by Royal Tiger were apparently placed by parties impersonating government agencies, banks, and utility companies, with other calls pertaining to purported credit card interest rate reduction offers.

The Public Notice also states that the Royal Tiger entities routed calls to Great Choice Telecom LLC, which is controlled by John Spiller, who was the subject of the second largest Forfeiture Order in the FCC's history (we summarized that 2021 decision here). The Enforcement Advisory then goes on to list the Royal Tiger entities' U.S.-based voice service customers "to aid industry stakeholders in connection with" their know-your-customer (KYC) processes and procedures.

C-CIST Label "Shines a Very Bright Light" on Bad Actors That Operate "In the Shadows"

The FCC's Fact Sheet explains that "[t]hreat 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" as a means of evading detection and enforcement. The Fact Sheet further explains that these bad actors frequently victimize consumers using information that they have harvested from data breaches and cyber intrusions, and they utilize spoofing technology and artificial intelligence voice cloning software to pose as trusted contacts. And the Bureau explains that these providers pose a particularized threat to the public because they are repeat offenders that "hid[e] behind a charade of shell companies" to evade accountability "and further their illicit conduct . . . ."

While the Fact Sheet notes that the Bureau may take a variety of enforcement actions, including cease-and-desist letters, Robocall Mitigation Database removal orders, and forfeiture orders against entities labeled as C-CISTs, the Bureau explains that the primary purpose of the classification is to "shine[] a very bright light on them for law enforcement, industry stakeholders, consumers, and businesses" because they thrive by operating in the shadows and behind shell companies. The Bureau intends to publicize C-CIST classifications on its webpage.

Industry Stakeholders Should Closely Monitor C-CIST Designations

Importantly, moreover, the Bureau expects industry to play a role in monitoring for C-CIST designees trying to penetrate their networks. Specifically, the Public Notice states that the C-CIST classification is intended to "provide industry stakeholders with information to enhance their [KYC] and ['Know Your Upstream Provider'] processes" because "[i]ndustry stakeholders are the first line of defense in keeping harmful traffic out of U.S. communications networks.

Accordingly, all voice providers should pay close attention to their KYC and onboarding practices, towards the goal of keeping C-CIST designees "out of U.S. communications networks." While the full scope of how the Commission intends to leverage this new classification tool remains unclear, the FCC's releases strongly suggest that the agency expects industry to take appropriate measures against C-CIST designees as appropriate. Voice providers should therefore take the time to evaluate their customer base and KYC protocols, and make improvements where necessary.

***

Wiley has a deep and experienced robocalling bench, and our experts handle federal and state policy issues, compliance with federal and state requirements, enforcement matters, and complex TCPA issues. For more information on any of these issues, please contact one of the authors listed on this alert.