January 5, 2026

Via ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
Washington, DC 20554

Re: CG Docket No. 17-59, *Advanced Methods to Target and Eliminate Unlawful Robocalls*; WC Docket No. 17-97, *Call Authentication Trust* Anchor; CG Docket No. 02-278, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*

The Computer & Communications Industry Association (CCIA)[1] is pleased to respond to the Federal Communications Commission (FCC or Commission) Further Notice of Proposed Rulemaking that seeks to update the robocall rules in order better to ensure that consumers know who is calling prior to answering a call.[2]

The STIR/SHAKEN framework has proved to be a significant advancement in ensuring that called parties have accurate identification of the ownership of originating number of incoming calls. But bad actors have established new ways of deceiving called parties. Moreover, as the Commission acknowledges, a "significant number of calls" are not protected by STIR/SHAKEN because they are carried by "portions of the national network [that] have not transitioned to IP." NPRM ¶ 7.

Recent survey data indicates that phone calls remain a commonly used means of perpetrating scams.[3] In 2023, 78% of mobile telephony users reported that they were victims of at least one scam.[4] This data indicates that the Commission's caller-identification regime has not entirely solved the problem of voice telephony being the conduit for scams.

In cases in which the A-level attestation is fully transmitted throughout the call transmission paths, STIR/SHAKEN is effective in combatting Caller ID ***spoofing***. However, this complete transmission is not guaranteed, and STIR/SHAKEN cannot prevent Man-in-the-middle (MITM)

[1] For more than fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. EchoStar is a CCIA member. The list of CCIA members is available at https://ccianet.org/about/members/.
[2] FCC 25-76 (rel. Oct. 29, 2025), published at 90 Fed. Reg. 56101 (Dec. 5, 2025), https://www.federalregister.gov/documents/2025/12/05/2025-22063/advanced-methods-to-target-and-eliminate-robocalls (visited Jan. 5, 2026).
[3] According to survey respondents, 37% of scams originated via phone calls. Morning Consult, *Scams and Protections* (June 2025), https://pro-assets.morningconsult.com/wp-uploads/2025/06/Google-x-Morning-Consult-US-Consumer-Scams-and-Protections-Blog-Report.pdf (visited Jan. 5, 2026).
[4] *A safer internet: policy recommendations for fighting scams and fraud together* (Nov. 14, 2024), https://blog.google/outreach-initiatives/public-policy/a-safer-internet-policy-recommendations-for-fighting-scams-and-fraud-together/ (visited Jan. 5, 2026).

call hijacking.[5] MITM call hijacking, the voice-call version of man-in-the-middle cyberattacks, occurs when a call's audio stream is intercepted. In this scenario, an unauthorized third party interrupts an IP-based voice transmission, blocks the calling party's audio from the transmission path, and takes on the persona of the calling party with the intent to deceive the called party. The originating-number information will remain unchanged, valid, and verified, but the media stream will have been compromised. This threat cannot be mitigated by the existing STIR/SHAKEN framework.

A hypothetical example of MITM hijacking: a call originated from a financial advisor to a potential client is hijacked by a bad actor who takes over the call in the guise of the advisor and deceives the called party into revealing their sensitive personal and financial data. The originating-number information will not have changed, but the voice on the phone definitely would have. The financial risks attendant with MITM call hijacking are obvious.

A growing variety of branded calling alternatives are available or soon will be introduced into the market to improve call authentication and verify caller identity to protect consumers from illegal and unwanted robocalls. These solutions work toward deterministically authenticating the calls at each occurrence, *i.e.*, converging verified caller identity, number ownership and the actual use of that number at each occurrence to confirm the authenticity of each specific call.

CCIA encourages the Commission to examine the ways that industry is creating and implementing solutions that provide consumers with additional, verified data about who is calling them. The Commission should monitor the development of these solutions and examine their effectiveness in combatting spoofing and hijacking throughout (*i.e.*, in every link of) all transmission paths. Bad actors that insert themselves into call paths rely on the goodwill of subsequent carriers to accept what might be fraudulent certifications. Industry efforts are in process to curb this activity.

The market for branded calling solutions remains nascent and should be allowed to develop further before being subject to regulatory mandates. In particular, industry should be encouraged at the outset to develop flexible, technology-neutral methods to enhance the identity verification framework and call authentication for business-branded callers. Verifying identities of individual callers is crucial for blocking the full panoply of scam and spam calls; it also involves myriad operational complexities. CCIA therefore suggests that the Commission should focus first on efforts to ensure enhanced identity vetting for enterprise callers, and then address issues surrounding identification of individual callers in a future proceeding after the industry has converged on best practices and technology.

The Commission has experience in working with industry to stamp out conduct by bad actors. This proceeding seems an appropriate opportunity to examine how industry is working to build upon the foundation set by the STIR/SHAKEN framework for the betterment of U.S. consumers.

[5] *E.g.*, AT&T, *Man in the Middle Scam* [*sic*], https://about.att.com/pages/cyberaware/ni/blog/man ("In the 'Man in the Middle' scam, the bad guy literally puts himself between you and a company where you have an account. In that middle position, he can convince the company he is you – and convince you he is the company.") (visited Jan. 5, 2026).

* * * *

CCIA appreciates the opportunity to respond on these matters and is available to provide any additional information that might be helpful to the Commission.

Sincerely,

Stephanie Joyce
Chief of Staff, Senior Vice President, and
Director of Litigation Center for the Connected Economy
Computer & Communications Industry Association (CCIA)