Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59

FURTHER NOTICE OF PROPOSED RULEMAKING IN
WC DOCKET NO. 17-97 AND CG DOCKET NO. 17-59

COMMENTS OF CONSUMER REPORTS

Consumer Reports applauds the FCC for taking steps to ensure that voice providers are taking appropriate steps to ensure that scam and spam callers are not able to access their networks, and to close loopholes that have allowed unwanted callers to plague Americans. In Consumer Reports' 2025 Cyber Readiness Report we discovered that 46% of Americans had encountered a scam, and 11% of those who encountered a scam said it began with a phone call.[1] These automated scam calls were 22% of the robocalls tracked by YouMail in March 2026.[2]

Americans are inundated with scam calls to the point where many will not answer a call from unknown numbers, leaving consumers to miss calls from their doctor's offices, pharmacies and other legitimate businesses. Reducing the volume of scam calls is paramount to restoring the utility of and trust in voice calling. The FCC in its NPRM on this topic acknowledges that the industry's self-regulation since the STIR/SHAKEN standards were implemented in 2020 have not succeeded, which has led to this inquiry.[3]

Consumer Reports strongly supports the FCC's efforts to strengthen the Know Your Upstream Provider (KYUP) requirements and believes the agency should close loopholes in the STIR/SHAKEN framework.

---

[1] Yael Grauer, Stacey Higginbotham, Jeff Landale. 2025 Cyber Readiness Report. Consumer Reports. October 1, 2025. https://innovation.consumerreports.org/2025-Consumer-Cyber-Readiness-Report.pdf
[2] YouMail. "Robocall Report April 2026". April 6, 2026. https://blog.youmail.com/2026/05/may-robocall-index-report-scam-calls-in-april-surge-decrease-month-over-month/
[3] Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls, Further Notice of Proposed Rulemaking, FCC-CIRC2605-01, WC Docket No. 17-97, CG Docket No. 17-59 (Apr. 29, 2026). *para.* 14

Strengthening KYUP Requirements

We agree with the agency's shift from focusing on preventing high volumes of illegal traffic to preventing illegal phone calls. Strategies such as this and the agency's decision to make the KYUP rules requirements as opposed to a set of best practices are essential steps to turn a flimsy policy that allowed millions of scam calls through into something with real teeth. We agree with the information collection requirements and compliance requirements, including requiring a check on the upstream provider's traceback history.

This compliance check and understanding of past behavior should be mandatory and subject to specific contracts, as opposed to a general statement noting that an upstream provider complies with all known rules. It is possible to see which upstream providers have a history of complaints or scams, and for voice service providers to then stop transmitting their traffic. But this doesn't necessarily happen today.

As recently as December 2025 the The Anti-Robocall Multistate Litigation Task Force sent letters to Lumen, Inteliquent, Bandwidth Inc. and Peerless accusing them of continuing to send illegal calls through their respective networks.

In the case of Inteliquent, the Task Force noted that at least 5,728 traceback notices were sent to Inteliquent since August 2022, which is after the Task Force first reached out about its concerns regarding Inteliquent's call traffic.[4] Bandwidth has received at least 2,319 of traceback notices since August 2022 after the Task Force first reached out about its concerns regarding Bandwidth's call traffic.[5]

Requiring a voice provider to understand traceback notices and how the upstream provider behaves, and requiring voice providers to police those bad actors by not allowing their calls through their networks is essential to ensuring that bad actors casually funneling scam calls through the network are stopped before those scams reach end consumers. The ineffective warnings sent by the Anti-Robocall Multistate Litigation Task Force in 2022 show how challenging it is for law enforcement to police scam calls.

---

[4]Letter from Tracy Nayer Special Deputy Attorney General Consumer Protection Division North Carolina Department of Justice to Stacy Graham at Inteliquent on December 3, 2025. Re: NOTICE from the Anti-Robocall Multistate Litigation Task Force Concerning Bandwidth, Inc.'s Continuing Involvement in Suspected Illegal Robocall Traffic. p.3.
https://web.archive.org/web/20260111134016/https://ncdoj.gov/wp-content/uploads/2025/12/State-AG-Task-Force-NOTICE-Letter-to-INTELIQUENT-Issued-12-03-2025.pdf

[5] Letter from Tracy Nayer Special Deputy Attorney General Consumer Protection Division North Carolina Department of Justice to Greg Rogers, Emily Harlan, Stephen Thayer at Bandwidth Inc. on December 3, 2025. Re: NOTICE from the Anti-Robocall Multistate Litigation Task Force Concerning Bandwidth, Inc.'s Continuing Involvement in Suspected Illegal Robocall Traffic. p.3.
https://web.archive.org/web/20260111134014/https://ncdoj.gov/wp-content/uploads/2025/12/State-AG-Task-Force-NOTICE-Letter-to-BANDWIDTH-Issued-12-03-2025.pdf

Adding the voice providers as a cop on the beat makes sense. They are more efficiently placed to take action against scam calls by preventing those that seek to make them from ever sending bad traffic through their networks. Requiring that they scrutinize their customers ensures an even playing field that prior efforts or merely setting these KYUP requirements as best practices would not.

Because the FCC is requiring voice providers act as a cop on the beat, CR agrees that providers should not be subject to liability under the Act or Commission rules for objectively reasonable decisions to refuse or discontinue service. We'd like to see providers take swift action when they become aware of an upstream provider sending suspicious traffic or receive complaints or tracebacks to a specific provider. CR advocates that a company should act quickly, implementing suspension as soon as is practicable but no later than two days when a bad actor is or bad behavior is suspected.

When an upstream provider is suspended, they should have an opportunity to appeal that suspension and have it adjudicated within five business days. Because a provider can make thousands of scam calls a day, every day counts when it comes to stopping the calls, but a legitimate business should also have a rapid appeals process to ensure that mistakes are corrected quickly. Scammers gravitate to the points of least friction, so they are unlikely to appeal, while a legitimate business will take the opportunity to clear their name.

Every voice provider should have a person or department in charge of complying with and enforcing the KYUP requirements within the organization. CR believes that because the industry has failed so spectacularly with regard to stopping scam calls so far, the FCC should not only mandate the KYUP information gathering and compliance requirements, but it should also require providers to obtain independent verification of their compliance through an independent auditor using generally accepted auditing practices.

The results of the audits should be filed to the Commission and made public. The audits should take place at least every two years. It's possible that after a five or ten-year time frame those audits may become less necessary and stopped at such time that the upstream providers become less of a vector for scam calls.

Strengthening STIR/SHAKEN

Requiring voice providers to know their customer is only half of the battle. The STIR/SHAKEN framework needs buttressing as well. The agency's plan to give the Governance Authority more power and rules while also building trust in the attestations associated with calls is essential.

The FCC should require that the Governance Authority include all of the KYUP information collection, compliance, and verification rules proposed by this order. When the Governance Authority cannot access that information or believes that the upstream provider will not comply with the STIR/SHAKEN rules then it should deny issuing a Service Provider Code (SPC) token.

And any provider unable to comply with the KYUP requirements should never become a Certificate Authority capable of issuing tokens.

The FCC also asked two important questions about Certificate Authorities; should they issue certificates that expire within a set period of time and if self-certification should be allowed. On the first, CR would like certificates to expire within two weeks. The technology industry has realized that the data shared in certificates becomes less secure over time and that many players that rely on certificates do a poor job of revoking them when their information is no longer valid.[6] Additionally based on a May 13, 2026, ex parte filing from the STI Governance Authority (STI-GA) Board and the Alliance for Telecommunications Industry Solutions (ATIS) the SPC tokens expire within two weeks.[7] There is no need to make this longer.

On the question of a voice provider acting as both a Certificate Authority and the recipient of a certificate from its own CA, Consumer Reports does not believe it should be allowed. There is an inherent conflict of interest, and the stakes are too high if a CA acts with impropriety issuing a certificate to a bad actor.

And much like with those who violate the KYUP requirements, those who commit fraud with the STIR/SHAKEN framework should see their tokens revoked or their ability to issue certificates terminated immediately by the Governance Authority. The Governance Authority can then review the action and determine if the token should be granted or Certificate Authority reinstated.

The other pillar of STIR/SHAKEN is the attestation associated with each call passed through the network. The current system is clearly not working. There are many calls that have the highest level of assertion that are still spam. These A-level calls are supposed to be calls where the service provider has authenticated the calling party and they are authorized to use the calling number. B-Level calls are those where a service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number.

But data already in the FCC's record show that too many A-level-attested calls are illegally spoofed calls. The FNPRM offers the assertions that "93.4% of robocall traffic from the most prolific robocall signers now carry A-level attestations," and "48 percent of illegal calls are A-attested."[8] Comments filed by the American Banking Association provided several examples of this including an analysis conducted for the ABA that conducted that of 12,900 calls that

[6] Stephen Davidson. "TLS Certificate Lifetimes Will Officially Reduce to 47 Days." DigiCert. May 16, 2025. https://www.digicert.com/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-days

[7] Letter from Tom Goode, General Counsel, ATIS, et al., to Marlene H. Dortch, Secretary, FCC, Attach. at 5 (filed. May 15, 2026) (ATIS May 15, 2026 Ex Parte).
https://www.fcc.gov/ecfs/document/105150795022052/2

[8] Letter from Keith Buell, General Counsel and Head of Global Public Policy, and Rebekah Johnson, Founder and Chief Executive Officer, Numeracle, to Marlene H. Dortch, Secretary, FCC, CG Docket 17-59, WC Docket 17-97, CG Docket 02-278, CG Docket 25-307, at 2 (filed Oct. 21, 2025)

illegally spoofed telephone numbers belonging to 47 large banks, retailers, and healthcare providers, more than half of the calls received an A-level or B-level attestation.[9]

The FCC believes that better codifying the rules around attestations and closing existing exemptions is the best way to improve the quality of attestations. We agree that stopping bad actors through the KYUP provider requirements should stop a lot of the fraud currently seen in attestations today, but believe that closing other gaps will leave scammers with fewer opportunities to squirm through.

We agree that the FCC needs to define improper attestation and formally prohibit voice service providers from improperly attesting that their calls are more trustworthy than are. The FCC's efforts to clarify ambiguous definitions and determine if pay-for-attestation schemes are undermining the framework are worthwhile.

We also agree that the FCC should remove the hardship exemption for companies that can not obtain a token. The FCC's own research indicated that companies that used the exemption did not indicate why they needed and in many cases improperly claimed the exemption.[10] We also agree with the FCC's determination that companies originating calls via satellite using NANP numbers are able to implement STIR/SHAKEN without undue hardship,[11] so this exemption should also be removed.

Consumer Reports is grateful that the FCC recognized that the work it did in 2020 was not sufficient to stop the scourge of scam calls. We support the agency's efforts to improve the STIR/SHAKEN framework, propose more stringent requirements on voice providers to know their upstream providers, and require those providers to act as a cop on the beat ensuring the quality of the traffic that goes through their networks.

---

[9] In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Dismissal of Outdated or Otherwise Moot Robocalls Petitions, CG Docket Nos. 17-59, 02-278, & 25-307, WC Docket No. 17-97, Comments of the Am. Bankers Ass'n et al., 22-24 (filed Jan. 5, 2026), https://www.fcc.gov/ecfs/document/10106019480304/1.

[10] Further Notice of Proposed Rulemaking, FCC-CIRC2605-01 *para*. 107

[11] Further Notice of Proposed Rulemaking, FCC-CIRC2605-01 *para*.108