National Consumer Law Center
Fighting Together for Economic Justice

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

Letter to JEC

Dear Lauren and Brandon,

Thank you for your interest in the problems caused by scam calls and texts. We hope that the information and ideas discussed when we met on May 16, 2025, were of use to you. With this letter, our goal is to provide additional background information and more specific recommendations to address unwanted and dangerous calls and texts.

I. Scope of the problem.

One of the best ways to see the scope of the problem caused by scam calls and texts is through the data compiled by companies which provide call blocking and answering services to millions of consumers, such as YouMail. This website illustrates the type and numbers of robocalls through April 2025 and is based on an extrapolation from calls routed to YouMail's thirteen million users. YouMail's statistics describe telemarketing and scam calls separately, as telemarketers typically maintain that they have consent and therefore their calls are legal, making it unclear whether calls that purport to be telemarketing are fraudulent. But both types of calls are unwanted.

The combined estimate of **monthly** calls for telemarketing and scam calls in April 2025 was **2.68 billion calls** (2.06 billion telemarketing and .62 billion scam). YouMail's longitudinal analysis indicates that the volume of robocalls to U.S. consumers has increased in 2025, reversing previous trends where robocalls had been stable or decreasing.

II. Money lost to scam calls and texts.

The FTC provides statistics about scam losses *reported* to various governmental agencies. The amounts lost are increasing year to year. In 2024, Americans reported losses of $12.5 billion from scams, with $470 million in reported losses from text scams and $948 million reported lost from scam calls. *Consumer Sentinel Network Data Book 2024*, at page 12. In 2023, consumers reported $10 billion in fraud losses with $372 million and $850 million attributable to text message and phone scams respectively. *Consumer Sentinel Network Data Book 2023* at pages 11-12.

However, as the FTC's data relies on consumers' reports of their losses it understates the magnitude of the problem. A January 2024 survey of approximately 2,000 individuals by The Harris Poll on behalf of the call blocking service Truecaller estimated that **56.2 million U.S adults lost over 25.4 billion** to scam calls in 2023. Regardless of exactly what dollar figure U.S. consumers lost to fraud, the data is clear—scam calls and texts impose significant and increasing losses.

III. Causes of scam calls and texts.

As explained in our report *Scam Robocalls: Telecom Providers Profit* on the causes of scam calls (pages 11-14), unlike the historical way telephone calls were transmitted, calls are now routed through a series of telecommunications providers in a call path that is governed by contractual agreements, with the provider receiving payment based on the number of minutes of connected calls upstream providers send through its network. The scam calls are generally processed into the telephone network by complicit providers who actually know—or consciously avoid knowing—that they are transmitting illegal calls.

One problem is that complicit providers deliberately mix scam calls with the flood of telemarketing calls, as well as alerts, reminders, and debt collection messages sent lawfully. This mixing of legal and illegal calls makes it much more difficult for terminating providers to label or block the scam calls accurately. And, when legal calls are mislabeled, the callers are quite upset. As a result, terminating carriers may be overly cautious about blocking and labeling and many scam calls successfully make it through the system to the subscribers.

The TRACED Act, passed by Congress in 2019, attempted to address scam calls by making the caller-IDs that accompany the calls more reliable. Pursuant to that law, the FCC instituted a caller ID authentication system referred to as Stir/Shaken, which requires that providers in the call path attach an attestation to the call signaling header that accompanies each call, indicating whether the provider transmitting the call knows the identity of the caller and whether the caller has a legal right to use the telephone number appearing as the caller-ID.

The FCC, the FTC, the terminating providers, and many people working in the communications field now recognize that often these attestations are virtually meaningless. First, many of the A-level attestations, which are supposed to indicate that the provider attesting to the call knows the identity of the caller and knows that the caller has a right to use the calling phone number, are simply false, and the fact that they are false is known or suspected by providers up and down the call path. Providers who knowingly assist scammers by giving them access to the network have shown a willingness to falsify attestations. Virtually none of these providers have faced enforcement actions as a result of their false attestations. As we suggest below, crafting meaningful consequences for providers who flout laws and regulations is essential.

Second, callers can anonymously and inexpensively purchase the temporary use of telephone numbers from complicit providers—generally VoIPs (Voice over Internet Protocol service

companies). The purchase or rental of temporary numbers technically provides the callers with the right to use the caller-IDs for those numbers. But when telemarketers and scammers can rotate through thousands of numbers a day, responsible providers downstream are unable to determine whether the calls coming from those numbers can be trusted. Additionally, generally the recipients of those calls are unable to reach anyone by calling the number back. As we have been advocating, eliminating the ability of illegal callers to rotate through telephone numbers is a key to eliminating many of these unwanted and illegal calls.

After passage of the TRACED Act, the FCC implemented the Robocall Mitigation Database (RMD) as a way to identify and police the providers transmitting calls into and through the U.S. telephone network. The intent was to ensure that all providers implement a system that identifies and avoids transmitting illegal voice traffic. The FCC's RMD regulation, 47 C.F.R. § 64.6305, prohibits providers from accepting and transmitting calls from upstream providers that have not registered in the RMD or that have registered but been de-listed pursuant to an enforcement action. There are now well over 8,000 registrations in the RMD, but these registrations are not reviewed or vetted in any meaningful way. Many contain false or misleading information, making it difficult for providers to determine whether an RMD entry reflects a legitimate company or has been fabricated by a provider that intends to transmit scam robocalls.

To skirt FCC regulations and enforcement efforts, many VoIP service companies that are based outside of the United States establish shell corporations within the country to appear on the RMD as domestic providers. These companies can originate internet-based telephone calls on behalf of callers located virtually anywhere in the world while misrepresenting to downstream providers that the calls are originated domestically. A search of the FCC's RMD shows a disproportionate number of registrants' business addresses are in Sheridan, Wyoming. This jurisdiction has been documented as a popular location to establish fraudulent shell corporations.

In December, 2024, the FCC threatened to remove 2,400 providers for failing to comply with the RMD registration requirements. Removal from the RMD is supposed to result in other providers refusing to accept call traffic from the removed provider, theoretically shutting the provider out of the United States' phone network. But when a provider runs into trouble, it simply submits a new entry into the RMD using a new name. Other than some basic information and a promise to comply with the applicable regulation, there are no meaningful cost or information barriers to registering new entities. Although the FCC requires a $100 application fee to register or annually update information in the RMD, there is no requirement that the payment come from the registrant or a financially responsible party. Shell corporations that transmit scam calls to the U.S. consumers are still able to register in the RMD without meaningfully identifying themselves, which means that the RMD is not an effective deterrent to fraudsters.

Furthermore, the FCC's enforcement regime relies on forfeiture penalties and removal from the RMD to incentivize compliance. However, in *AT&T Corp. v. Federal Communications Comm'n* ,

135 F.4th 230 (5th Cir. 2025), the Fifth Circuit recently held that the FCC's current procedures for assessing penalties are unconstitutional because they do not allow the respondent a jury trial in an Article III court. Also, to remove a provider from the RMD for transmitting illegal calls in violation of the FCC's regulations, the FCC must go through an entire enforcement action to prove the specific violations. The resources required for case-by-case enforcement are tremendous, meaning that only a small percentage of bad-actors ever face consequences.

IV. What can be done to stop scam calls and texts.

There are lots of good regulations and statutes on the books, and we have suggestions for additional rules and laws that would be useful. But the bottom line is that without enforcement new rules and statutes are mostly meaningless. We believe that in this environment, the likely best answer is new requirements that are self-executing or can be easily and quickly enforced by state and federal agencies against domestic providers. The goal is to create a set of requirements that would be relatively simple to apply but would create meaningful incentives for providers to comply with the rules.

Licensing and bonding. The act of transmitting telephone calls and texts into the U.S. telephone network should be a privilege, in which only qualified and responsible entities are permitted to engage. Providers should be required to hold a valid license to transmit messages into the network.

This privilege should be no less strict than the requirements for driving on public highways, which requires a valid driver's license. Similarly, the right to be a barber, a real estate agent, a lawyer, or a healthcare professional, are all contingent on holding a valid license. These professions require passing tests, which are intended to be sufficiently difficult to eliminate unqualified applicants. Instead of a test, voice and text service providers could be required to post bonds.

Requiring a bond would force a provider to either post a substantial sum or convince a third-party bond company that it is a legitimate company that does not intend to transmit fraudulent calls to U.S. consumers. A requirement for significant bond amounts would also provide an avenue for enforcement authorities to recover funds on behalf of consumers who were injured by a provider's transmission of scam calls. If a significant bond exists to compensate injured consumers, enforcers would be guaranteed that their investment of significant time and energy in bringing an enforcement action would result in a meaningful recovery for consumers.

Current FCC regulations regarding the RMD are similar to a licensing requirement, in that the FCC can pursue removal from the RMD to effectively prohibit a provider from accessing the U.S. phone network. Formalizing the RMD's requirements into a statutory licensing scheme would tighten the filing requirements and could introduce a bond requirement. These measures would effectively eliminate providers' ability to effortlessly establish new shell corporations and refile after being removed from the RMD.

Provide a Clear Path for FCC Enforcement. As stated above, recent precedent indicates that the FCC does not have a legal pathway to assess civil penalties. Fixing this issue to restore the FCC's enforcement ability is of critical importance. Congress should specifically authorize the FCC to file actions for civil penalties in federal district courts.

Increasing Resources for Public Enforcement. Government enforcement authorities' ability to identify providers complicit in the transmission of scam calls exceeds their ability to take legal action to stop them. This is illustrated by a recent letter from the North Carolina Attorney General to Lingo, a VoIP, warning it to stop processing illegal calls. The letter was sent on behalf of the Anti-Robocall Multistate Litigation Task Force, in which all 50 states and the District of Columbia participate.

The letter from the NC AG notes that the Industry Traceback Group run by U.S. Telecom had issued **630 traceback notices** to Lingo about "high-volume illegal and/or suspicious robocalling campaigns concerning SSA government imposters, financial impersonations, utility disconnects, Amazon suspicious charges, student loans, and others, ..." The letter notes that there had been 105 traceback notices issued since the Task Force had first warned Lingo in 2022. Further, "each traced call is representative of a large volume of similar illegal and/or suspicious calls." Indeed, as the letter points out, the FCC had issued a Notice of Suspected Illegal Traffic in February 2024, yet the calls kept being transmitted by Lingo to U.S. subscribers.

Based on information the Task Force obtained from Lingo through a Civil Investigative Demand, the letter estimates that *193.1 million* scam robocalls in just two categories – Amazon/Apple imposter calls and SSA/IRS imposter calls -- are attributable to Lingo. Yet, neither the FCC, the FTC, nor the state AGs in all 50 states, have sufficient governmental resources to *stop* these tens of millions of scam calls from being delivered to U.S. telephone subscribers. We recommend providing additional resources so that enforcement authorities can take more robust action to stop scam calls.

Access to Numbering Resources. As discussed above, callers' ability to procure temporary access to phone numbers anonymously on a secondary market significantly undercuts the goals of the TRACED Act, and the FCC's implementation of STIR/SHAKEN. Temporary access to phone numbers also facilitates fraud. Restricting temporary access to numbering resources, particularly if coupled with record keeping requirements to ensure that number resellers know their customers, could improve caller ID authentication and help consumers avoid scam calls.

Requiring licensing and bonding, fixing and increasing government enforcement actions, and tightening access to numbering resources are not perfect solutions to the problems of scam calls and texts and unwanted telemarketing calls. But they would go a long way towards mitigating the harm consumers continue to suffer.

Thank you for your consideration of our ideas.

Sincerely,

Patrick Crotty

Senior Attorney

Margot Saunders

Senior Attorney