FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Improving Customer Service and Protecting Consumers through Onshoring	)	**CG Docket No. 26-52**
	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	**CG Docket No. 17-59**
	)	
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act	)	**CG Docket No. 02-278**
	)	
	)	
Empowering Broadband Consumers Through Transparency	)	**CG Docket No. 22-2**
	)	

Comments of

National Consumer Law Center
on behalf of its low-income clients

Public Knowledge

National Association of Consumer Advocates

Electronic Privacy Information Center

Consumer Action

Consumer Federation of America

National Consumers League

and

Consumer Reports

Table of Contents

Comments

Introduction and Summary

These Comments, submitted by the National Consumer Law Center (NCLC) on behalf of its low-income clients, and joined by Public Knowledge, the National Association of Consumer Advocates, the Electronic Privacy Information Center, Consumer Action, the Consumer Federation of America, the National Consumers League, and Consumer Reports, are in response to the Notice of Proposed Rulemaking and Further Notices of Proposed Rulemaking released by the Federal Communications Commission (Commission or FCC) on March 27, 2026,[1] and published in the Federal Register on April 23, 2026.[2] **We strongly support the Commission's proposal to require a telemarketing provider to post a substantial bond or equivalent security as a condition of registering in the Robocall Mitigation Database (RMD). This will help to ensure that scammers do not gain access to the U.S. telephone network.**

The Commission's commitment to addressing scam calls and the increasing consumer losses they cause has never been more important. Calls and text messages are a leading contact method for scams and generate higher median losses than any other contact method.[3] Low-income subscribers, such as older Americans on fixed incomes, can least afford to lose their savings to scammers, yet older Americans consistently have the highest median losses.[4] The Commission's leadership in addressing illegal calls is laudable and much needed.

---

[1] FCC, Notice of Proposed Rulemaking in CG Docket No. 26-52; Tenth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; Third Further Notice of Proposed Rulemaking in CG Docket No. 22-2 (adopted March 26, 2026, released March 27, 2026) (NPRM), https://docs.fcc.gov/public/attachments/FCC-26-16A1.pdf.

[2] https://www.federalregister.gov/documents/2026/04/23/2026-07960/improving-customer-service-and-protecting-consumers-through-onshoring.

[3] Federal Trade Commission Consumer Sentinel Network, Reports and Amount Lost by Contact Method, *Consumer Sentinel Network Data Book 2024*, at pg. 12

[4] Id. at pg. 13.

The Commission's NPRM astutely recognizes that scam calls proliferate because they are profitable for providers[5] and that "[t]here is an obvious need to take the profit out of these calls."[6] Enforcement actions leading to financial penalties against providers that knowingly allow scam calls to transit their networks are powerful disincentives that can deter providers from tolerating illegal traffic. However, enforcement actions have little effect on individuals who can effectively hide behind shell companies, which are businesses established without revealing their true owners that mask the identities and assets of criminal scammers. The Commission's proposal that providers post a bond as a condition of filing in the Robocall Mitigation Database (RMD) could address this problem. Requiring a surety bond, certificate of deposit, or irrevocable letter of credit that can be drawn on to pay a forfeiture or judgment arising from transmission of an illegal call will ensure that RMD filers are more than hollow shell companies. Posting such a security requires disclosing the identity of a responsible party to a third-party surety or financial institution, which would help eliminate the anonymity that scammers depend on and ensures that meaningful assets are reachable to pay for harms caused by their calls.

In section I of these comments, we describe how criminals can gain access to the U.S. phone network on an anonymous basis and with minimal investment of resources by using shell companies to set themselves up as voice over internet protocol (VoIP) providers. In section II we explain how a bond requirement will make it more difficult for these criminals to maintain their anonymity and will ensure that identifiable assets are available to address harms caused by fraudulent or otherwise illegal call traffic. In section III we discuss how a bond requirement could be structured to be fair

[5] NCLC has long agreed with this assessment. *See* National Consumer Law Center and Electronic Privacy Information Center, Scam Robocalls: Telecom Providers Profit (June 2022), https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf.
[6] NPRM at ¶ 68.

and effective. Finally, in section IV we identify sources of legal authority for implementing a bond requirement.

I. Criminals Use Shell Companies to Evade Accountability for Transmitting Scam Calls.

Scammers know that the more difficult they are to identify, the more difficult they are to prosecute. This need for anonymity shapes the tactics criminals use to perpetrate scams. There are many ways to gain access to the U.S. phone network without providing meaningful identifying information, but when anonymous access is coupled with the ability to place large volumes of calls at low costs it dramatically increases the amount of harm criminals can cause in a short time. The Commission has noted that VoIP telephone service is disproportionately associated with unlawful calls because it provides "high-volume, rapid-fire, calling [as] a cost-effective way for bad actors to find susceptible targets."[7] The Commission further noted that the "low barriers to entry" in the VoIP market contribute to the proliferation of VoIP providers and exacerbate illegal robocalling.[8]

VoIP's low barriers to entry enable anonymous shell companies to set themselves up as "imposter VoIP providers" – entities that pretend to be VoIP providers servicing legal callers but are actually criminal operations making high volumes of calls on their own behalf. These businesses are created through third-party services and headquartered at virtual offices or P.O. boxes, making it difficult or impossible to identify the individuals responsible for the company's fraudulent or otherwise illegal call traffic. The Industry Traceback Group has noted that imposter VoIP providers are a known source of harmful call traffic, stating: "[i]llegal robocallers are developing more complex

[7] FCC, Report to Congress on Robocalls and the Transmission of Misleading or Inaccurate Caller Identification Information, December 23, 2025. https://docs.fcc.gov/public/attachments/DA-25-1100A1.pdf.
[8] *Id.*

and sophisticated strategies to evade detection and law enforcement, for instance **by creating shell companies and imposter providers.**"[9]

Services that facilitate the creation of imposter providers operate in plain sight – openly offering to establish U.S. telecommunications companies in a short time for customers who pay relatively small amounts through difficult to trace payment mechanisms such as cryptocurrency. For instance, "TelComplance LLC" (sic) d/b/a TelcoCompliance advertises a service that lets customers "Launch Your Telecom Business in the U.S. with Full Compliance."[10] The company accepts "Flexible Payment Methods" including the cryptocurrencies Bitcoin and Tether.[11] It also claims to complete registrations quickly, boasting "7-14 business days" for STIR/SHAKEN registration.[12] A package of services offered for $2,000 includes: "WY Company Registration, 1st Year Agent Service, 1st Year DC Agent, EIN Registration, 499 Filing, OCN Filing, STI-PA Filing, 1 Year STI-CA Cert w Peeringhub, 1 Year 499A Filing" and for a separate price "IPES Registration" to "Become an IPES operator and register your own numbers."[13] The company provides no identifying information about itself beyond its website and a telephone number, making it difficult for investigators to subpoena information about the company's clients. The company, despite claiming to be an LLC, does not disclose the state in which it is registered, and based on a search of Westlaw public records, does not appear to be registered in any state. The company's stated phone number is also listed on a webpage for "International Carrier Exchange Limited," that provides various other contact information including a Hong Kong post office box number.[14] This seemingly related entity offers

[9] US Telecom – The Broadband Association, Letter to Loyaan Egal (March 24, 2023) (emphasis added), *available at*: https://docs.fcc.gov/public/attachments/DOC-399306A5.pdf.
[10] TelcoCompliance, About Us, https://www.telcompliance.com/#about (last accessed May 18, 2026).
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] One Penny SIM, 1psim Support, https://1psim.com/

international SIM cards and other products and services including "T-Mobile Bulk SMS."[15] This sounds suspiciously like an offer to send text messages through a SIM-farm[16] comprised of T-Mobile telephone numbers. It is entirely possible that companies which facilitate scam calls assist criminals by both setting up imposter VoIP providers and making calls through SIM-farms. This would provide redundancy and increased scale – making criminal operations more harmful and harder to disrupt.

TelcoCompliance's offer to establish a Wyoming company for its clients is not a coincidence. Wyoming has become a notorious haven for shell companies, though Delaware and Nevada laws allow for similarly anonymous business formation.[17] Wyoming companies are well represented in the RMD. For instance, one Wyoming address, 30 N. Gould St. in Sheridan, Wyoming, with a reputation for serving as the nominal address for operations of dubious legality or outright scams,[18] is well represented in the RMD. A recent search for "Gould" in the RMD produced a list of over fifty registrants. A search for Wyoming addresses in the RMD shows hundreds of additional providers. Though the disproportionate number of Wyoming companies

---

[15] *Id.*

[16] A SIM-farm is an array of SIM cards connected to devices which allow sending and receiving of voice calls or text messages.

[17] See Woodman, Spencer, International Consortium of Investigative Journalists, "Millions in Covid relief funds went to shadowy companies registered at a Wyoming storefront that hundreds of thousands of firms used as an address" (March 4, 2025), *available at* https://www.icij.org/investigations/pandora-papers/millions-in-covid-relief-funds-went-to-shadowy-companies-at-a-wyoming-storefront-that-hundreds-of-thousands-of-firms-used-as-an-address/ (last accessed May 18, 2026); Satter, Raphael, Reuters, "How cybercriminals are using Wyoming shell companies for global hacks" (Dec. 13, 2023), *available at* https://www.reuters.com/technology/cybersecurity/how-cybercriminals-are-using-wyoming-shell-companies-global-hacks-2023-12-12/ (last accessed May 18, 2026).

[18] Lodewyk, Georgia, The Sheriden Press Via Wyoming News Exchange, "30 N. Gould St. businesses blur lines of what it means to be a Sheridan business" (Nov. 29, 2024, and updated Jan. 5, 2026), *available at* https://www.wyomingnews.com/news/local_news/30-n-gould-st-businesses-blur-lines-of-what-it-means-to-be-a-sheridan/article_66d94fa4-ae8b-11ef-b606-7bad3d698a86.html (last accessed May 18, 2026).

registered in the RMD is not evidence that any particular Wyoming filer is engaged in fraud, it does suggest that RMD filing requirements alone are not sufficient to prevent the use of shell companies to form imposter VoIP providers that transmit fraudulent robocalls.

We are mindful that the Commission has also initiated proposed rules to strengthen Know-Your-Customer (KYC) and Know-Your-Upstream Provider (KYUP) requirements. Better KYC and KYUP rules will also help to keep scammers out of the U.S. phone network; however, these policies will work best in concert with, and not supplant, measures such as a bond requirement that can prevent scammers from forming imposter VoIP providers and attempting to slip through KYC and KYUP practices to gain access to the U.S. phone network through legitimate intermediate and gateway providers.

II. A Bond Requirement Will Make It More Difficult to Establish Imposter VoIP Providers and Help to Ensure That Assets are Available to Pay for Harm Caused by Illegal Calls.

The Commission should require that providers post a surety bond, irrevocable letter of credit, or certificate of deposit as a condition of registering in the RMD and file proof in their RMD filing. This will work in concert with the Commission's rules at 47 C.F.R. § 64.6305(g) to prohibit accepting call traffic from any provider who has not complied with the security requirement. Providers that do not submit proof that they have complied with this security obligation and have not obtained a waiver, or demonstrated they are exempt from the obligation, should not be allowed to complete the registration process or should be removed from the RMD in a summary fashion so that other providers are forbidden from transmitting their call traffic. Existing RMD registrants should be given a reasonable deadline to file proof that they have satisfied the requirement.

A bond or similar security requirement to file in the RMD will serve two purposes. First, having to obtain a surety bond, letter of credit, or certificate of deposit will make it more difficult for a criminal to anonymously create an imposter VoIP provider because a third party will need to act as

a surety or hold assets in the registrant's name. Sureties typically require identifying information about a bond principal, the entity that is required to obtain the bond, so that if the principal's conduct triggers a claim against the bond and the surety surrenders the bond amount, then the surety can identify an individual or adequately capitalized company against whom it can seek subrogation. Sureties also typically assess a bond applicant's personal credit score and the financial stability of the bonded company to determine the appropriate cost or premium associated with the bond.[19]

Bond premiums for telemarketing bonds, which operate in a similar manner to the bond requirement we propose, typically cost between 1% and 10% of the bond amount.[20] Over twenty states require some form of telemarketing bond, including the three most populous states, Texas, Florida and California, which require telemarketing bonds of $10,000, $50,000, and $100,000, respectively.[21] The prevalence of professional bond requirements demonstrates that there is a competitive market that is equipped to service communications providers required to file proof of a surety bond in the RMD. Essentially, a bond requirement would, at little or no cost to the Commission, outsource vetting RMD applicants to third parties with a significant financial interest in ensuring that criminals are unable to file RMD certifications.

---

[19] See, SuretyBonds.com, What is a Surety Bond?, How Much Does It Cost to Get a Surety Bond, https://www.suretybonds.com/what-is-a-surety-bond

[20] See e.g. https://floridasuretybonds.com/set-price-telemarketing/ ("The cost of a Telemarketing Bond is a premium that generally ranges from 1% to 5% of the total bond amount required by your state. . . However, applicants with lower credit scores or new call centers without a financial track record may see premiums range from 5% to 10% or may be required to post collateral. Ultimately, the price depends on your personal credit score and the financial stability of your business.")

[21] See NCLC, Federal Deception & Abuse Law (5th ed. 2024) at Appendix D, *updated at* www.nclc.org/library; *see also* State of California Department of Justice, Telephonic Seller Registration, https://oag.ca.gov/consumers/general/telreg ("All telephonic sellers are required to have a $100,000 bond issued by a surety company admitted to do business in California. The bond is required to cover consumer losses.").

Letters of credit or certificates of deposit would fulfill a similar function because financial institutions are required to observe federal anti-money laundering (AML) and counter terrorism (CT) financing regulations when issuing such instruments. The KYC requirements imposed by AML and CT laws and regulations provide an incentive for financial institutions to scrutinize providers who elect to use this form of security. Allowing the use of alternate forms of security could provide greater flexibility for providers with varying sizes and resources. A certificate of deposit would give RMD filers the option to use their own money instead of paying a premium to a surety and earn interest while the funds act as security. A letter of credit would not even require the RMD filer to tie up funds to fulfill the requirement and may be a good option for larger providers who have established a trusted relationship with a financial institution. In both cases, the Commission should require that the financial institution backing the RMD filer be present in the United States, to ensure that U.S. AML and CT regulations apply and so that a claim against the certificate of deposit or letter of credit can be made without the risk of foreign laws and regulations interfering with the claim.

Requiring a surety bond, certificate of deposit, or irrevocable letter of credit as a condition of filing in the RMD will ensure that if a provider knowingly transmits illegal call traffic, there will be assets available to pay a forfeiture or judgment arising from the harmful calls. Voice service providers, including intermediate and gateway providers, can be held liable for knowingly transmitting calls that violate the Telephone Consumer Protection Act, the Truth in Caller ID Act, the Telemarketing Sales Rule (TSR), and state statutes governing unfair and deceptive acts and practices.[22] However, holding a voice service provider liable for harmful calls is largely meaningless if

[22] *Off. of Att'y Gen. v. Smartbiz Telecom LLC*, No. 22-23945-CIV, 2024 WL 4251895, at *4 (S.D. Fla. Sept. 19, 2024) (citing In the Matter of Rules & Reguls. Implementing the Tel. Consumer Prot. Act of 1991, 7 F.C.C. Rcd. 8752, ¶ 54 (1992); *Arizona v. Michael D. Lansky L.L.C.*, No. CV-23-00233-TUC-CKJ, 2024 WL 3657129 (D. Ariz. May 8, 2024); *Indiana v. Startel Commc'n LLC*, No.

it does not have the assets to pay a forfeiture, judgment, or settlement. Requiring that RMD filers post a surety bond, certificate of deposit, or letter of credit that can be drawn against to pay for harms caused by transmitting illegal calls ensures that at least some assets are available to satisfy the company's liability. Additionally, the information individuals generally have to submit to obtain the required security means that there will most likely be identifiable individuals who can potentially be held liable for the provider's transgressions.

Telemarketing bonds again provide useful examples of how a bond requirement ensures that assets are available to pay for harms related to illegal calls. In one case, the Federal Trade Commission (FTC) and the Florida Attorney General sued several companies and their principals for violations of the FTC Act, the TSR, and the Florida Deceptive and Unfair Trade Practices Act arising from an illegal credit card interest rate reduction scam.[23] The defendants subsequently settled the claims for individual liability, agreeing to pay a combined total of $425,000, and a default judgment was entered against the corporate defendants.[24] Both the individuals' consent judgments and the default judgment entered against the corporate defendants included language stating: "This Order and Permanent Injunction is the result of a government agency action on behalf of injured purchasers of Defendants' debt relief product or service and may serve as the basis to recover any surety bond, letter of credit, certificate of deposit, or other form of security filed with the Florida

321CV00150RLYMPB, 2022 WL 22702954, (S.D. Ind. Sept. 9, 2022); *see also Mey v. All Access Telecom, Inc.*, No. 5:19-CV-00237-JPB, 2021 WL 8892199, at *5 (N.D.W. Va. Apr. 23, 2021) ("Defendant was involved in the placing of the telephone calls because it knowingly allowed fraudulent calls to transit its network.").

[23] See FTC Summary of Action for GDP Network LLC (YF Solution), Last updated May 22, 2023, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3137-gdp-network-llc-yf-solution.

[24] Operators of Credit Card Interest Rate Reduction Scam Permanently Banned from Debt Relief Business Under Settlement with the FTC and Florida Attorney General, February 28, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/02/operators-credit-card-interest-rate-reduction-scam-permanently-banned-debt-relief-business-under

Department of Agriculture and Consumer Services ("FDACS"). Restitution may be paid from any such surety bond, letter of credit, certificate of deposit, or other form of security filed with the FDACS."[25] Pursuant to this language, the plaintiffs were able to make claims on the defendants' telemarketing bonds and return more than $557,000 to injured consumers.[26] The bulk of the additional $132,000 paid to injured consumers in excess of the individual defendants' $425,000 contribution came from claims against the corporate defendants' telemarketing bonds. This example shows that bond requirements can meaningfully improve outcomes for consumers harmed by illegal calls.

III. The Commission Should Structure a Bond Requirement to be Fair and Effective.

We urge the Commission to promulgate rules setting forth a bond requirement that are procedurally fair while effectively restraining fraudulent or otherwise illegal call traffic. There are numerous bonding requirements under state and federal law that suggest reasonable ways in which the Commission could structure a bond requirement to fulfill these goals. State telemarketing bond requirements are especially relevant as they are also generally concerned with limiting illegal call traffic and providing relief for consumers harmed by illegal calls. Drawing from relevant examples, we discuss how the Commission's rules should address who is subject to the bond requirement, how to establish compliance with the requirement, and how claims against a bond should be lodged and paid.

[25] Order, https://www.ftc.gov/system/files/ftc_gov/pdf/gdpordergracedepaz.pdf; Order, https://www.ftc.gov/system/files/ftc_gov/pdf/gdporderdefault_judgmentgdpnetwork.pdf.
[26] FTC Sends More Than $557,000 to Consumers Harmed by Credit Card Interest Rate Reduction Scam, May 22, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-sends-more-557000-consumers-harmed-credit-card-interest-rate-reduction-scam.

A. Entities Subject to the Requirement

The Commission should apply a bond requirement broadly to RMD filers[27] since the Commission's rules allow for the suspension, amendment, or waiver of the requirement upon a showing of good cause.[28] Entities that believe there are compelling reasons they cannot or should not be required to post a security to file in the RMD are free to state their case to the Commission through a request for a suspension, waiver, or amendment.

Should the Commission deem it necessary to exempt a class of RMD filers from the bond requirement preemptively, then we suggest that the Commission consider exempting RMD filers who provide rural telephone service and participate in the Universal Service Fund High Cost program or the United States Department of Agriculture Rural Utilities Service program. Providers who participate in these programs are subject to federal audits and will generally be identifiable and are unlikely to knowingly transmit illegal calls to subscribers as they may face suspension or termination from these programs.

B. Establishing Compliance with the Requirement

The Commission's rules should set forth the size of the security required to be posted to comply with the requirement, the forms the security may take, and how the RMD filer must provide proof that it has complied with the requirement to post the security. First, we recommend that, as a baseline, the Commission require security in an amount substantially in excess of $100,000. Several state telemarketing laws require sellers to post a surety bond or other form of security worth at least

[27] All voice service providers and intermediate providers, including gateway providers, VoIP resellers, mobile virtual network operators, and subsidiaries or affiliates of filers that independently meet the definition of a voice service provider or intermediate provider, must file in the RMD. See Robocall Mitigation Database Frequently Asked Questions for Filers, https://www.fcc.gov/sites/default/files/rmd-faq.pdf.

[28] 47 C.F.R. § 1.3.

$100,000.[29] This indicates that high value surety bonds are commercially available and not prohibitively expensive. A security of over $100,000 also provides a meaningful amount to pay restitution to subscribers harmed by illegal calls. We believe that a baseline requirement of $250,000 is justified given that the median losses caused by scam calls and texts are $1,500 and $1,000 respectively,[30] and imposter VoIP providers can place millions of calls per day. On average, a scammer would only need to defraud 167 subscribers before causing over $250,000 in harm, making this a conservative estimate of the necessary security.

A larger security, perhaps as high as $1,000,000 would better protect subscribers, and the Commission should consider increasing the amount of security required for certain types of RMD filers. For instance, if an RMD filer receives a high volume of tracebacks over a long period of time, fails to respond to tracebacks, or provides false information in response to a traceback, then that provider represents a greater risk of transmitting illegal call traffic which justifies a larger security for the privilege of continuing in business. Other factors, such as receipt of a complaint from State Attorneys General or a history of violating other rules imposed by the Commission, should also be considered when determining whether to increase the amount of security required.

Next, the Commission's rules should specify the acceptable forms of security. Federal law sets forth requirements which guarantee that surety bonds, or alternative eligible obligations as

---

[29] *See, e.g.*, Cal. Bus & Prof Code § 17511.12(a) ("Every telephonic seller shall maintain a bond issued by a surety company admitted to do business in this state. The bond shall be in the amount of one hundred thousand dollars ($100,000) in favor of the State of California for the benefit of any person suffering pecuniary loss in a transaction commenced during the period of bond coverage with a telephonic seller who violated this chapter."); Ariz. Rev. Stat. Ann. § 44-1274(A) ("A seller shall maintain a bond of one hundred thousand dollars issued by a surety company duly authorized to do business in this state."); W. Va. Code § 46A-6F-302(a) ("A separate bond in the amount of $100,000 may be filed for each telemarketing location, including each principal office and each branch office thereof, or a single bond in the amount of $500,000 may be filed for all locations of the telemarketer.").

[30] Federal Trade Commission Consumer Sentinel Network, Reports and Amount Lost by Contact Method, *Consumer Sentinel Network Data Book 2024*, at pg. 12

discussed in 31 U.S.C. § 9303, provide meaningful security. We suggest that the Commission allow RMD filers to satisfy a security requirement by attaching a bond executed by a surety listed as a Certified Company by the Bureau of the Fiscal Service[31] to its RMD filing. The requirement to use a Certified Company helps to ensure that the surety is legitimate. Also, requiring the executed bond to be filed in the RMD will make it easy to verify that the RMD filer has fulfilled the security requirement. Providers that fail to attach the executed bond would be visible to the Commission and the members of the public, who could report non-compliance to the Commission using the RMD-Reporting@fcc.gov email address. If an RMD filer instead elects to give an eligible obligation within the scope of 31 U.S.C. § 9301(2) as security instead of a surety bond, then the filer should be required to submit the eligible obligation directly to the Commission for approval and file a statement noting acceptance of the collateral from an applicable bureau in the RMD as proof.

Additionally, we suggest that the Commission allow, in lieu of attaching an executed surety bond, RMD filers to attach an irrevocable letter of credit issued for the benefit of the filer by a bank whose deposits are insured by an agency of the Federal Government or a certificate of deposit in a financial institution insured by an agency of the Federal Government, which may be withdrawn only on the order of the Commission or an appropriate bureau, except that the interest may accrue to the RMD filer. Some state telemarketing laws allow for this form of security,[32] and it may provide additional flexibility in satisfying the requirement, particularly if the Commission elects not to exempt large, public facing voice service providers.

[31] https://fiscal.treasury.gov/about-us/doing-business-with-fiscal-service/surety-bonds/list-certified-companies.

[32] *See, e.g.*, Fla. Stat. § 501.611(1)(b)-(c).

C. Claims Against Security and Payment of Claims

We recommend that the Commission require that all surety bonds designate the Commission as obligee, but that the Commission's rules also permit governmental agencies and injured subscribers to make claims against the bond or other security posted by the RMD filer. State telemarketing laws often allow both the bond obligee as well governmental agencies and harmed individuals to make claims against a surety bond or other security.[33] We recommend that the Commission's rules specify that a final judgment entered by any state or federal court arising from the transmission of one or more calls, including text messages, that caused harm due to fraud, misrepresentation, or a violation of specified statutes constitute sufficient grounds to require the surety to pay the judgement amount from the bond. We suggest that the Commission should allow judgments obtained under the Telephone Consumer Protection Act, Telemarketing Consumer Fraud and Abuse Prevention Act and Telemarketing Sales Rule, the Truth in Caller ID Act, and state statutes governing unfair and deceptive acts and practices to serve as sufficient proof to trigger a draw against the bond or other security. This will ensure that the legal tools available to State

[33] *See, e.g.*, Fla. Stat. § 501.611(4) ("The department or a governmental agency, on behalf of an injured purchaser or a purchaser herself or himself who is injured by the applicant, may bring and maintain an action to recover against the bond, letter of credit, or certificate of deposit."); Ala. Code § 8-19A-10(d) ("The division or any governmental agency, on behalf of any injured purchaser or any purchaser himself or herself who is injured by the bankruptcy of the applicant or his or her breach of any agreement entered into in his or her capacity as a licensee, may bring and maintain an action to recover against the bond, letter of credit, or certificate of deposit."); Ark. Code Ann. § 4-99-107(b)(2)(C) ("A person suffering injury or loss by reason of any violation of this chapter shall be paid the proceeds of the bond, or shall be paid under the terms of any order of a court of competent jurisdiction obtained by the Attorney General or prosecuting attorney as a result of any violation of this chapter."); Cal. Bus & Prof Code § 17511.12(a) ("The bond shall be in the amount of one hundred thousand dollars ($100,000) in favor of the State of California for the benefit of any person suffering pecuniary loss in a transaction commenced during the period of bond coverage with a telephonic seller who violated this chapter. The bond shall include coverage for the payment of the portion of any judgment, including a judgment entered pursuant to Section 17203 or 17535, that provides for restitution to any person suffering pecuniary loss, notwithstanding whether the surety is joined or served in the action or proceeding.").

Attorneys General and other enforcement authorities who bring legal actions against VoIP providers are able to recover on behalf of their constituents. If the RMD filer elected to post a certificate of deposit, a letter of credit, or another eligible obligation, then the financial institution or the Commission holding the security should pay a qualifying judgment up to the extent of the security.

Requiring proof in the form of a forfeiture or judgment owed to the Commission, or a judgment arising from illegal call traffic owed to governmental or private entity, to support a claim against a surety bond or other security will guarantee procedural fairness. We recommend that the Commission's rules recognize that a stipulated judgment or default judgment, as well as a litigated judgment, can act as proof supporting a bond claim. The Commission's forfeiture process as well as state and federal court procedural rules have significant due process protections built in. These protections will ensure that communications providers will not be held liable and forfeit their surety bond or other security without sufficient cause. The Commission could also consider crafting a less formal procedure that still allows RMD filers to dispute complaints about illegal traffic and provides procedural fairness. A less formal procedure would provide a benefit to consumers and government enforcement authorities by expediting restitution for harms caused by the transmission of illegal calls. The Commission should also consider allowing a complaint regarding illegal call traffic resolved in the complainant's favor under 47 U.S.C. § 208 to serve as sufficient proof to support a bond claim.

IV. Legal Authority Supporting a Bond Requirement

The Commission has legal authority under 47 U.S.C. §§ 201(b), 202(a), 227(b) and (c), and ancillary authority, to impose a bond requirement on service providers as a condition of filing in the RMD. Creating imposter VoIP providers for the purpose of evading accountability for knowingly transmitting illegal call traffic is unquestionably an unjust and unreasonable practice, and the Commission's regulatory authority under 47 U.S.C. § 201(b) can and should be used to address such

practices. Additionally, allowing providers to avoid liability for transmitting illegal calls by hiding behind shell corporations or otherwise hiding assets would give undue and unreasonable advantage to scammers and unlawful traffic in violation of 47 U.S.C. § 202(a).

The Commission also has authority under 47 U.S.C. § 227(b)(2) to implement the requirements of § 227(b), which restrict autodialed and prerecorded or artificially voiced calls. A security requirement ensures these restrictions cannot be easily circumvented, which is an important aspect of implementation.

Finally, the Commission has authority under 47 U.S.C. § 227(c)(2) to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object. A bond requirement will deter the transmission of illegal telemarketing calls and fits well within the scope of this delegation of regulatory authority.

Conclusion

We applaud the Commission for its efforts to combat fraudulent and otherwise illegal calls and thank the Commission for the opportunity to comment on this important issue.

Respectfully submitted this 26th day of May 2026, by:

Patrick Crotty
Senior Attorney
National Consumer Law Center
1001 Connecticut Ave., NW
Washington, D.C. 20036
pcrotty@nclc.org