



NATIONAL  
ASSOCIATION OF  
ATTORNEYS GENERAL

PRESIDENT

**Ellen F. Rosenblum**  
Oregon  
Attorney General

November 12, 2024

PRESIDENT-ELECT

**John Formella**  
New Hampshire  
Attorney General

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554**

VICE PRESIDENT

**William Tong**  
Connecticut  
Attorney General

In the Matter of )

Improving the Effectiveness of )  
the Robocall Mitigation Database )

WC Docket No. 24-213

IMMEDIATE PAST  
PRESIDENT

**Dave Yost**  
Ohio  
Attorney General

Amendment of Part 1 of the )  
Commission’s Rules, Concerning )  
Practice and Procedure, )  
Amendment of CORES )  
Registration System )

MD Docket No. 10-234

**Brian Kane**  
Executive Director

**REPLY COMMENTS OF FORTY-SEVEN (47)  
STATE ATTORNEYS GENERAL**

**I. Introduction**

1850 M Street NW  
12th Floor  
Washington, DC 20036  
(202) 326-6000  
www.naag.org

The undersigned State Attorneys General (“State AGs”) submit these Reply Comments in response to the public notice issued by the Wireline Competition Bureau and Office of the Managing Director.<sup>1</sup> The public notice seeks comment on the Federal Communications Commission’s (“Commission”) proposals to increase accountability and accuracy among filings in the Robocall Mitigation Database (“RMD”).

<sup>1</sup> See Notice of Proposed Rulemaking, *Improving the Effectiveness of the Robocall Mitigation Database*, WC Docket No. 24-213, *et al.*, Adopted August 7, 2024 (“August 2024 Notice”).

These proposals include procedural measures that the Commission could adopt to promote the highest level of diligence when providers submit required information to RMD; technical solutions that the Commission could use to identify and require correction of data discrepancies in filings; measures the Commission could implement to increase accountability for providers that submit inaccurate and false information to the RMD or fail to update their filings when the information they contain changes; and other procedural steps the Commission could require to increase the effectiveness of the RMD as a compliance and consumer protection tool.

The RMD is an essential resource in State AGs' efforts to combat illegal robocalls. However, too often the information submitted by providers to the RMD is clearly false or inaccurate and demonstrates contempt for the Commission's requirements and the consumers those requirements protect. In our investigative and enforcement efforts, State AGs have encountered facially deficient RMD entries and mitigation plans similar to those of the twelve (12) providers the Commission removed from the RMD on February 22, 2024.<sup>2</sup> These deficiencies include false, incomplete, or misleading contact information, blank or inapplicable mitigation plans, and representations which are contradicted by other FCC filings or publicly available sources.

State AGs applaud the Commission's efforts to improve the quality of RMD entries and increase accountability for providers who exploit our residents by facilitating fraudulent or otherwise illegal robocalls. The RMD can and should be more than a mere formality that bad actors glibly disregard. The undersigned State AGs write in support of the Commission's proposals to improve this vital tool in the fight to protect American consumers.

---

<sup>2</sup> Removal Order, *In the Matter of Viettel Business Solutions Company et al.*, EB-TCD-23-0034918 *et al.*, Adopted February 22, 2024.

## II. Additional Procedural Measures Would Improve the Accuracy of RMD Entries

State AGs agree with the Commission that “[a] review of filings in the [RMD] indicates that, among some providers, diligence is lacking.”<sup>3</sup> While some deficient RMD filings are undoubtedly attributable to malfeasance on the part of bad actors, the Commission should also consider embedding clarifying information into the process of creating RMD entries to guide providers that may have difficulty interpreting the Commission’s rules.

For instance, to complete an RMD certification form, providers must manually enter whether they are a “foreign voice service provider.”<sup>4</sup> The Commission has defined a foreign voice service provider as “any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country.”<sup>5</sup> State AGs have found that providers have been inconsistent in their interpretation of this definition. For example, some providers who are headquartered outside of the United States and can originate foreign voice calls that terminate within the United States do not state that they are a foreign voice service provider in the RMD because they list a domestic mailing address or purchase access to a domestic third-party’s Voice over Internet Protocol switching platform to transmit calls. Linking or otherwise directing providers to interpretive guidance as they complete this portion of the RMD certification form could assist them in making accurate and consistent certifications.

Inaccurate RMD information undercuts the effectiveness of the Commission’s other efforts to combat illegal robocalls. In particular, the Industry Traceback Group (“ITG”), the Commission’s

---

<sup>3</sup> August 2024 Notice at ¶ 13.

<sup>4</sup> *Id.* at ¶ 7.

<sup>5</sup> 47 C.F.R. § 64.6300(c).

appointed consortium that traces suspected illegal calls to their origin, uses the foreign voice service provider certification to assign providers' roles in tracebacks. Inaccurate certifications can cause the ITG to erroneously designate a provider as a point of entry or a foreign point of departure in tracebacks of suspected illegal calls. These inconsistencies in how providers are labeled in tracebacks complicates State AGs' investigative efforts using traceback data. Interpretative guidance on applying the Commission's definitions could improve the accuracy of the RMD and other robocall mitigation efforts.

Similarly, guidance on the meaning of undefined terms could also improve the accuracy of information in the RMD. State AGs have found that providers have inconsistently certified required information such as their business address. Some providers may supply the address of a commercial mail receiving agency or a virtual office that may receive general corporate correspondence, while others supply the physical address of their headquarters, their network operations center, or a similar location where individuals charged with corporate decision making regarding robocall mitigation can be reached. Providing specific guidance to providers on what contact information should be listed in the RMD could limit misunderstandings and improve the usefulness and consistency of RMD entries.

Also, State AGs agree with the Commission's proposal to adopt a rule requiring providers to update any information submitted to the Commission Registration System<sup>6</sup> ("CORES") within 10 business days of any changes to that information. Harmonizing the information in CORES and

---

<sup>6</sup> CORES is the system the FCC uses to facilitate the assignment of FCC Registration Numbers ("FRNs") to all persons and entities seeking to do business with the FCC. 47 C.F.R. § 1.8002(a). As obtaining an FRN is a precondition to filing in the RMD—or doing any other business before the Commission—information submitted to CORES in order to obtain an FRN should be consistent with information submitted to the RMD, and any discrepancy indicates that, at a minimum, providers did not exercise due care in their filings.

the RMD will reduce confusion by improving the accuracy of information in both databases, which will benefit both providers and law enforcement agencies that rely on the RMD to identify potential bad actors using, or attempting to use, United States communications networks for illegal purposes. Any incidental administrative costs required to update CORES information within 10 business days are justified by the important ends that the information serves.

Furthermore, as the Commission's rules already require that providers keep CORES information current,<sup>7</sup> setting a deadline of 10 business days simply reinforces an existing requirement with an ample deadline for updating information and is unlikely to impose any significant cost on already compliant providers. State AGs also support the Commission imposing this requirement on all FCC Registration Number ("FRN") registrants, regardless of whether they are business or individual registrants. The difference between small businesses and individuals is not always meaningful and having unequal requirements for business and individual FRN holders could encourage gamesmanship.

State AGs also support the Commission's use of multi-factor authentication and requiring that filers obtain a PIN each time they submit information to the RMD. These procedural measures help to eliminate unauthorized access as a reason for inaccurate filings and help to establish that filers have personal knowledge of information entered in the RMD. State AGs' enforcement authority often extends to individuals who directly participate in malfeasance or have knowledge of a corporation's bad acts and the ability to control the corporation's conduct. Requiring a corporate officer or controlling individual to "submit additional information and certifications to obtain a PIN that must be used to submit [an RMD] certification"<sup>8</sup> helps to provide a connection

---

<sup>7</sup> 47 C.F.R. § 1.8002(b)(2).

<sup>8</sup> August 2024 Notice at ¶ 21.

between corporate policies and individuals, which will contribute to effective enforcement. Obtaining a PIN for each filing would ensure that a responsible individual is clearly associated with each representation a company makes in the RMD and would also eliminate the need to affirmatively relinquish the PIN if an individual leaves employment with the provider.

Additionally, State AGs have found that certain providers submit only a registered agent's contact information or a non-monitored phone number in the RMD. In some instances, the registered agents listed do not have knowledge of the company, which complicates efforts to investigate potentially illegal call traffic associated with the provider. Requiring an individual to supply contact information including, but not limited to, a name and verified email address or phone number to obtain a PIN will help to ensure that law enforcement can quickly reach a knowledgeable individual regarding the provider's call traffic, should it be necessary to do so. Privacy issues arising from the collection of individual contact information are outweighed by the benefits of effective enforcement. Filers need only provide contact information used for business purposes, which does not raise significant privacy concerns.

Further, State AGs support the Commission's proposal to require that providers remit a filing fee when submitting filings to the RMD.<sup>9</sup> Imposing a fee will discourage filings by bad actors, as payment methods frequently provide a useful pathway to discover identifying information for parties that could otherwise remain anonymous. State AGs believe that the Commission should consider requiring providers to file or renew their RMD submissions periodically and remit a filing fee only for these submissions, rather than each time an RMD entry is edited. Providers should not be disincentivized to make frequent updates to RMD filings to

---

<sup>9</sup> The Commission estimates that the filing fee would be \$100, which would cover the costs of resources to perform compliance assessments. *See* August 2024 Notice at ¶ 29.

ensure that information is as current as reasonably possible. Currently, the RMD contains entries which have not been updated in years, and requiring a filing fee to maintain an entry in the RMD would naturally eliminate entries which no longer reflect active market participants.

Analogous fees charged for annual renewal of access to the Federal Do Not Call Registry have proven to be accepted and workable requirements and demonstrate the feasibility of requiring a periodic application or renewal fee in this context. The Commission currently requires providers to file annual certifications documenting their compliance with Consumer Proprietary Network Information rules.<sup>10</sup> The Commission could adopt a similar process for RMD updates and compliance with RMD rules and add an annual filing fee requirement.

State AGs also support the Commission's proposal to apply the red-light rule to RMD filings. State AGs have seen considerable abuse of "free trial" access to communications networks. The red-light rule would prevent unscrupulous providers from filing RMD entries and transmitting robocalls for a limited time even though those providers have no intention of providing a traceable payment to the Commission.

### **III. Increased Use of Data Validation Tools Will Improve RMD Filings**

Nearly blank RMD entries, clearly fictitious information, and disingenuous false or copied robocall mitigation plans are unfortunately commonplace in the RMD and can be addressed by imposing technical validation steps on filings. State AGs support the Commission's proposals to prevent or exclude filings that cannot be validated against external or publicly accessible information sources or that are inconsistent with information in CORES filings. In particular, State AGs have encountered false address information that could be prevented or flagged for further review by comparing the provider's address to a United States Postal Service ("USPS") database.

---

<sup>10</sup> See 47 C.F.R. § 64.2009(e).



Although the Commission should ensure that providers have the ability to input additional information that may not be present in a USPS database, such as suite numbers or other clarifications, preventing RMD filings by providers who do not, or cannot, provide a valid address will significantly improve the quality and usefulness of the RMD.

Additionally, the Commission should consider flagging residential addresses, commercial mail receiving agencies, and other address types that are not indicative of an actual business presence at the address. Similarly, automatically checking that corporate filers have active corporate status in their state of incorporation would provide further assurance that an RMD filer is a legitimate enterprise.

Both law enforcement and providers rely on the information in the RMD and would benefit from technical enhancements to the RMD filing process that prevent entering blank, inaccurate, misleading, or contradictory information. Similarly, providers' robocall mitigation plans supply important information that both law enforcement and other providers evaluate. Implementing technological verification tools to detect and prevent the submission of blank, incomplete, inapplicable, misleading, or even fictitious mitigation plans will meaningfully enhance the reliability of the RMD and its consumer protection purpose. State AGs support the Commission's proposals to reject facially insufficient RMD submissions in the first instance and to provide filers whose entries become inaccurate with notice and an opportunity to cure. This approach balances rigorous enforcement with procedural fairness.

#### **IV. False and Inaccurate Information in the RMD Warrants Serious Penalties**

State AGs agree that submitting false or inaccurate information to the RMD implicates the Commission's comparable rules concerning misrepresentation and lack of candor and justifies the highest possible penalty. Ongoing non-compliance allows providers to profit from facilitating



fraudulent or otherwise illegal calls, and State AGs support the Commission in assessing penalties on a continuing basis so that providers' gains from illegal activity cannot offset the cost of a one-time penalty.

The accuracy of RMD entries is entirely within providers' control, and the obligation to protect consumers from fraudulent and illegal calls should be treated with the utmost seriousness. Other authorities, such as the Secure Telephone Identity Governance Authority, defer to the Commission's guidance and interpretations regarding problematic conduct in the telecommunications industry. False or inaccurate RMD filings undermine the Commission's efforts to combat illegal robocalls by requiring implementation of the STIR/SHAKEN call authentication framework when those RMD filings play a role in determining providers' eligibility to obtain service provider code tokens. State AGs encourage the Commission to demonstrate that disregarding consumer protection safeguards like the RMD filing requirements is a serious breach of trust that warrants significant penalties.

#### **V. Permissive Blocking for Facially Non-Compliant Providers is Warranted**

State AGs agree that willful violation of the Commission's rules requiring providers to describe the steps they are taking to avoid carrying and transmitting illegal robocalls supports a presumption that no such steps are being taken and that the provider is doing nothing to stop illegal traffic. The Commission's proposal to allow 48 hours for a provider with a facially deficient plan to cure the deficiency and avoid permissive blocking is appropriate and more than fair.

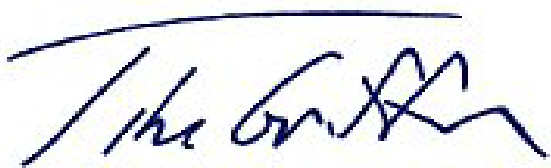
State AGs also support a safe harbor from liability under the Communications Act or the Commission's rules for providers that engage in permissive blocking when the Wireline Competition Bureau flags another provider in the call stream for non-compliance with the Commission's RMD rules. This will encourage providers to take quick action, which is warranted

to protect consumers. In the event that the provider cures the non-compliance, the Commission's proposal that the Wireline Competition Bureau take down the flag applied to the RMD filing and notify any providers that have commenced permissive blocking to cease such blocking is reasonable. State AGs support limiting permissive blocking to facially non-complaint providers, including providers that over-redact mitigation plans. State AGs believe that delegating authority to the Wireline Competition Bureau is appropriate given the ministerial nature of these determinations.

## VI. Conclusion

The RMD is currently one of the most important sources of information available for anti-robocall enforcement actions. Improving the accuracy of its information, holding owners and executives accountable, and providing appropriate penalties for providers that disregard the Commission's requirements will help to ensure that the RMD continues to function as a key resource and invaluable consumer protection tool. State AGs applaud and support the Commission's proposals.

**RESPECTFULLY SUBMITTED BY 47 STATE ATTORNEYS GENERAL**



Tim Griffin  
Arkansas Attorney General



Kwame Raoul  
Illinois Attorney General



Josh Stein  
North Carolina Attorney General



Dave Yost  
Ohio Attorney General

Steve Marshall  
Alabama Attorney General

Treg R. Taylor  
Alaska Attorney General

Kris Mayes  
Arizona Attorney General

Rob Bonta  
California Attorney General

Phil Weiser  
Colorado Attorney General

William Tong  
Connecticut Attorney General

Kathleen Jennings  
Delaware Attorney General

Brian Schwalb  
District of Columbia Attorney General

Ashley Moody  
Florida Attorney General

Christopher M. Carr  
Georgia Attorney General

Anne E. Lopez  
Hawaii Attorney General

Raúl Labrador  
Idaho Attorney General



Todd Rokita  
Indiana Attorney General



Brenna Bird  
Iowa Attorney General



Kris Kobach  
Kansas Attorney General



Russell Coleman  
Kentucky Attorney General



Liz Murrill  
Louisiana Attorney General



Aaron M. Frey  
Maine Attorney General



Anthony G. Brown  
Maryland Attorney General



Andrea Joy Campbell  
Massachusetts Attorney General



Dana Nessel  
Michigan Attorney General



Keith Ellison  
Minnesota Attorney General



Lynn Fitch  
Mississippi Attorney General



Andrew Bailey  
Missouri Attorney General

Aaron D. Ford  
Nevada Attorney General

John M. Formella  
New Hampshire Attorney General

Matthew J. Platkin  
New Jersey Attorney General

Raúl Torrez  
New Mexico Attorney General

Letitia James  
New York Attorney General

Drew H. Wrigley  
North Dakota Attorney General

Gentner Drummond  
Oklahoma Attorney General

Ellen F. Rosenblum  
Oregon Attorney General

Michelle Henry  
Pennsylvania Attorney General

Peter F. Neronha  
Rhode Island Attorney General

Alan Wilson  
South Carolina Attorney General

Marty Jackley  
South Dakota Attorney General

Jonathan Skrametti  
Tennessee Attorney General

Sean D. Reyes  
Utah Attorney General

Charity Clark  
Vermont Attorney General

Jason S. Miyares  
Virginia Attorney General

Patrick Morrissey  
West Virginia Attorney General

Joshua L. Kaul  
Wisconsin Attorney General

Bridget Hill  
Wyoming Attorney General