



PRESIDENT

Tom Miller
Iowa
Attorney General

PRESIDENT-ELECT

Josh Stein
North Carolina
Attorney General

VICE PRESIDENT

Ellen F. Rosenblum
Oregon
Attorney General

IMMEDIATE PAST PRESIDENT

Karl A. Racine
District of Columbia
Attorney General

Al Lama
Acting Executive Director

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

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

**REPLY COMMENTS OF FIFTY-ONE (51)
STATE ATTORNEYS GENERAL**

I. Introduction

The undersigned State Attorneys General (“State AGs”) submit these Reply Comments in response to the public notice issued by the Consumer and Governmental Affairs and Wireline Competition Bureaus,¹ seeking comment on the Federal Communication Commission’s (“Commission”) proposals to expand rules focusing on gateway providers “to cover other providers in the call path, along with additional steps to protect American consumers from all illegal calls, whether they originate domestically or abroad.”²

¹ See *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 22-37 (May 19, 2022) [hereinafter *May 2022 FNPRM*].

² *Id.* at 64 ¶ 157.

Like the Commission, many of our offices report that “unwanted calls, including illegal robocalls, are consistently . . . a top source of consumer complaints.”³ Moreover, as the Commission recognizes, illegal robocalls cost law enforcement, the telecommunications industry, and, most importantly, our constituents, approximately \$13.5 billion every year.⁴ In 2021, American consumers, including seniors, persons with disabilities, and other vulnerable populations, were bilked out of \$830 million via fraud perpetrated over the phone and/or through text messages.⁵ In many cases, the perpetrators of this fraud are foreign actors gaining access to the U.S. phone network through international gateway providers.⁶ Based upon consumer complaints filed with our offices, these fraudulent, foreign-originated robocalls often involve caller ID spoofing of U.S.-based phone numbers. Yet, without assistance from willing domestic providers to deliver illegal robocalls, these calls would never reach Americans.

³ See *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 22-37, at 2 ¶ 4 (October 1, 2021) [hereinafter *October 2021 FNPRM*].

⁴ *Id.*; see also *id.* at 4 ¶ 9 (finding that when an entity spoofs a large number of calls in a robocall campaign, it causes harm to subscribers, to consumers receiving the spoofed calls, and to the terminating carriers who incur increased costs due to consumer complaints).

⁵ This number is reached by combining amounts lost to fraud by phone call (\$699 million) with amounts lost by text (\$131 million). See Federal Trade Commission, *Fraud Reports by Contact Method, Year: 2021*, FTC CONSUMER SENTINEL NETWORK (data as of June 30, 2022) <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/LossesContactMethods> (Loss & Contact Methods tab, Year 2021).

⁶ *October 2021 FNPRM*, *supra* note 3, at 12–13 ¶¶ 26, 27, 28 (recognizing that a large portion of unlawful robocalls made to U.S. telephone numbers originate outside of the U.S.; that most foreign-originated fraudulent traffic uses a U.S. number in the caller ID field that is transmitted and displayed to the U.S. call recipient; that illegal, foreign-originated robocalls can only reach U.S. consumers after they pass through a gateway provider that is unwilling or unable to block such traffic; and that the Commission’s Enforcement Bureau has repeatedly identified gateway providers as playing a key role in routing illegal robocall traffic into the U.S.).

The May 19, 2022, *Gateway Provider Report and Order*⁷ was an important step toward cutting the strings that form the nets that these illegal robocallers cast over Americans. However, illegal robocalls continue to reach consumers, and the next logical step is to require *all* U.S.-based intermediate⁸ providers, whether they are accepting and routing a call as a gateway provider or as a non-gateway intermediate provider, to authenticate Caller ID information consistent with STIR/SHAKEN for calls carrying a U.S. number in the caller ID field, and to implement many of the meaningful robocall mitigation practices that are now required of gateway providers.

To this end, and consistent with recent Reply Comments filed with the Commission by State AGs related to these issues,⁹ State AGs support the Commission’s current proposals to extend STIR/SHAKEN authentication protocols to all U.S. intermediate providers as described in the May 2022 FNPRM.¹⁰ Illegal robocallers depend upon a relatively small number of unscrupulous

⁷ *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59 & Fifth Report and Order in WC Docket No. 17-97, FCC 22-37, at 10 ¶ 19 (May 20, 2022).

⁸ For use in these Reply Comments, we adopt the Commission’s proposed definition of “intermediate provider” to mean “any entity that [carries] or processes traffic that traverses or will traverse the [public switched telephone network (PSTN)] at any point insofar as that entity neither originates nor terminates that traffic.” See *May 2022 FNPRM*, *supra* note 1, at 3 ¶ 4 n.1.

⁹ See, e.g., Reply Comments of Fifty-One (51) State Attorneys General, *Numbering Policies for Modern Communications*, WC Docket No. 13-97, *Telephone Number Requirements for IP-Enabled Service Providers*, WC Docket No. 07-243, *Implementation of TRACED Act Section 6(a)–Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket No. 20-67, *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, filed Nov. 15, 2021 (supporting the Commission’s proposals to reduce access to numbering resources by potential perpetrators of illegal robocalls); Reply Comments of Fifty-One (51) State Attorneys General, *Call Authentication Trust Anchor*, WC Docket No. 17-97, filed Aug. 9, 2021 [hereinafter *August 2021 Reply Comments*] (encouraging Commission to require small voice service providers that flood the U.S. telephone network with illegal robocalls to implement STIR/SHAKEN caller ID authentication as soon as possible); Reply Comments of Fifty-One (51) State Attorneys General, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, *Call Authentication Trust Anchor*, WC Docket No. 17-97, filed Jan. 10, 2022 [hereinafter *January 2022 Reply Comments*] (encouraging Commission to require gateway providers that flood the U.S. telephone network with illegal robocalls to implement STIR/SHAKEN caller ID authentication as soon as possible).

¹⁰ *May 2022 FNPRM*, *supra* note 1, at 64 ¶¶ 158, 160–73.

VoIP providers who integrate their call traffic into the larger body of legitimate call traffic where it becomes more difficult to detect and stop. STIR/SHAKEN authentication protocols require calls to carry information which identifies the provider who originated the call and attests to whether that provider knows the subscriber who placed the call and if they know the subscriber is authorized to use the calling number. Importantly, requiring all intermediate providers to comply with STIR/SHAKEN so that they no longer strip this information from calls will both assist downstream voice service providers who can prevent known sources of illegal robocalls from abusing their networks,¹¹ and assist State AGs in targeting those individuals and companies that are responsible for, and participate in, an enterprise that robs Americans of the freedom to answer their phones and continues to cause billions of dollars in losses.

Because we are mindful that there is no “silver bullet” solution to curb the scourge of illegal and fraudulent robocalls, State AGs also fully support the Commission’s proposal to expand to all domestic providers the requirement to implement affirmative and effective mitigation practices. The Commission’s current proposal to require all U.S.-based intermediate providers to implement both STIR/SHAKEN authentication protocols and robocall mitigation practices are common-sense next steps in the effort to meaningfully mitigate illegal and fraudulent robocall traffic on a larger scale.

¹¹ The FCC permits call-blocking programs based on reasonable analytics including “information about the originating provider, such as whether it has been a consistent source of unwanted robocalls and whether it appropriately signs calls under the SHAKEN/STIR framework.” Declaratory Ruling and Third Further Notice of Proposed Rulemaking, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, *Call Authentication and Trust Anchor*, WC Docket No. 17-97, adopted June 6, 2019, at ¶ 35.

II. The Commission Should Extend Current STIR/SHAKEN Gateway Obligations to All Domestic Intermediate Providers

The Commission proposes extending the call authentication requirements beyond gateway providers to all domestic intermediate providers in the call path.¹² STIR/SHAKEN provides increased protections for consumers against receiving illegally spoofed calls, but only with true end-to-end, universal implementation of STIR/SHAKEN protocols by all voice service providers.¹³ If providers along the call path are obligated to refuse calls from providers that fail to comply with STIR/SHAKEN, it will be more difficult, and costly, for bad actors to find providers that are still willing to route their illegal and fraudulent call traffic. This is a win for consumers, since “illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”¹⁴

Relatedly, State AGs respectfully urge the Commission to adopt its proposed rules to establish deadlines for intermediate providers to implement STIR/SHAKEN authentication obligations as soon as possible.¹⁵ As the Commission recognizes in its proposal,¹⁶ many intermediate providers accept call traffic as gateway providers and should have already

¹² *May 2022 FNPRM*, *supra* note 1, at 63 ¶ 158.

¹³ *August 2021 Reply Comments*, *supra* note 9, at 3; *see also* Reply Comments of Fifty-One (51) State Attorneys General, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, *Call Authentication Trust Anchor*, WC Docket 17-97, filed Aug. 23, 2019, at 4–6 (supporting the Commission in taking regulatory action against those providers who fail to implement STIR/SHAKEN and supporting the prohibition of domestic voice service providers from accepting voice traffic from any other providers who fail to comply with STIR/SHAKEN); Reply Comments of Thirty-Five (35) State Attorneys General, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket Number, 17-59, filed Oct. 8, 2018, at 4–5 (urging the Commission to explore ways to encourage all domestic and international service providers to aggressively implement STIR/SHAKEN).

¹⁴ CHRIS FRASCELLA & MARGOT SAUNDERS, SCAM ROBOCALLS TELECOM PROVIDERS PROFIT 18 (Nat’l Consumer L. Ctr. And Electronic Privacy Info. Ctr. 2022) (quoting Statement of Commissioner Geoffrey Starks, *Call Authentication Trust Anchor*, WC Docket No. 17-97, FCC 21-105, filed Sept. 30, 2021).

¹⁵ *May 2022 FNPRM*, *supra* note 1, at 66 ¶ 169.

¹⁶ *Id.* at 65 ¶¶ 165, 166.

implemented STIR/SHAKEN pursuant to the Commission’s May 19, 2022 *Order*.

Further, the absence of a mandate that obligates all U.S.-based intermediate providers to implement STIR/SHAKEN overlooks the lessons learned and reflected in the Commission’s prior decision to reconsider an initial two-year blanket extension¹⁷ that expanded the original June 30, 2021 STIR/SHAKEN industry-wide implementation deadline to June 30, 2023 for a subset of small voice service providers. As the Commission learned from its previous experience, the longer this tier of providers is excused from having to shoulder the same authentication responsibilities as those providers above them in the call path, the more heightened the risk that an insulated subset of small voice service providers will continue to accept and route “an especially large amount of [illegal] robocall traffic.”¹⁸ State AGs have been consistent in our call for the Commission to require voice service providers along the call path to implement STIR/SHAKEN without delay, and we do so again here.¹⁹

¹⁷ In March 2021, pursuant to the mandates of the TRACED Act, voice service providers had until June 30, 2021, to implement STIR/SHAKEN. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3257–58 ¶¶ 32–35 (rel. Mar. 31, 2020); 47 CFR § 64.6301. Small voice service providers were granted a two-year extension to June 30, 2023. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1876 ¶ 38 (rel. Oct. 1, 2020).

¹⁸ *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Third Further Notice of Proposed Rulemaking, FCC 21-62, at 2 ¶ 1 (May 21, 2021).

¹⁹ *See, e.g.,* Reply Comments of Fifty-One (51) State Attorneys General, *Numbering Policies for Modern Communications*, WC Docket No. 13-97, *Telephone Number Requirements for IP-Enabled Service Providers*, WC Docket No. 07-243, *Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket No. 20-67, *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, filed Nov. 15, 2021 (supporting the Commission’s proposals to reduce access to numbering resources by potential perpetrators of illegal robocalls); *August 2021 Reply Comments, supra* note 9 (encouraging Commission to require small voice service providers that flood the U.S. telephone network with illegal robocalls to implement STIR/SHAKEN caller ID authentication as soon as possible); *January 2022 Reply Comments, supra* note 9 (encouraging Commission to require gateway providers that flood the U.S. telephone network with illegal robocalls to implement STIR/SHAKEN caller ID authentication as soon as possible).

III. The Commission Should Extend Certain Robocall Mitigation Duties to All Domestic Providers in the Call Path

The Commission further proposes to obligate all domestic intermediate providers to adopt affirmative mitigation programs, including a 24-hour traceback response requirement, mandatory call blocking, and a general duty to mitigate illegal robocalls.²⁰ State AGs support each of these proposals as set out by the Commission. Consistent application of these obligations for all providers in the call path would close the loophole²¹ that allows some providers to abdicate or shirk what should be a shared responsibility among providers to mitigate the continued deluge of illegal robocalls.

A. 24-Hour Traceback Requirement

Currently, all gateway providers must respond fully to all traceback requests from the Commission, civil or criminal law enforcement, as well as the industry traceback consortium, within 24 hours of receiving a request.²² The Commission proposes (1) extending this requirement to all domestic intermediate providers in the call path,²³ and (2) seeks feedback on whether to “adopt an approach to traceback based on [the] volume of requests received, rather than position in the call path, or size of provider” in a “tiered” approach.²⁴ The proposed tiered approach to traceback response obligations would require providers with, for example, fewer than 10 traceback requests per month to respond “in a timely manner” without the need to respond within 24 hours, between 10 and 99 traceback requests per month to “maintain an average 24-hour response,” and 100 or more traceback requests a month to consistently respond to tracebacks within 24 hours.

²⁰ *May 2022 FNPRM*, *supra* note 1, at 63 ¶ 158.

²¹ *Id.* 68–69 ¶ 175.

²² *Id.* at 30 ¶ 65.

²³ *Id.* at 69 ¶ 177.

²⁴ *Id.* at 69 ¶ 179.

State AGs unequivocally support the extension of the 24-hour traceback response requirement to all domestic intermediate providers. As the Commission recognizes, “traceback is an essential part of identifying the source of illegal calls,” wherein “time is of the essence . . . particularly for foreign-originated calls where . . . law enforcement may need to work with international regulators to obtain information from providers outside of U.S. jurisdiction.”²⁵ However, State AGs discourage the Commission from adopting a tiered approach to the timelines for compliance with the traceback requirement.

Instead, State AGs support uniformly expanding the existing 24-hour response requirement for traceback obligations on gateway providers to all domestic providers. A uniform requirement is clear and equitable. Further, the 24-hour response time is not overly burdensome to providers in the context of the crisis this country experiences daily in the tsunami of illegal robocalls. Moreover, the information that is required for a provider to comply with a traceback request can be found by accessing data that is automatically generated for every call routed to and from every provider in the normal course of business. This data is used by providers as a basis for billing, among other things.²⁶ Yet, since these records are not retained for consistent periods of time or with any predictability or regularity across providers in the industry, a shortened timeframe for traceback responses for all providers will increase the likelihood that this data, which is both critical and ephemeral, will be preserved to enable providers to respond to time-mandated,

²⁵ *October 2021 FNPRM*, *supra* note 3, at 21 ¶ 52.

²⁶ NATIONAL ASSOCIATION OF ATTORNEYS GENERAL, COMMENTS OF FORTY-THREE (43) STATE ATTORNEYS GENERAL: TELEMARKETING SALES RULE (16 C.F.R. PART 310—NPRM) (PROJECT NO. 411001) 6 (2022) [hereinafter *Aug. 2022 FTC Comments*] (supporting the FTC’s proposed amendments to the Telemarketing Sales Rule that would impose additional recordkeeping requirements on telemarketers and sellers, including retention requirements for call detail records).

ministerial requests designed to curtail illegal robocalls.²⁷ For these reasons, State AGs support extending a uniform 24-hour traceback requirement to all domestic intermediate providers.

B. Mandatory Blocking Following Commission Notification and Mandatory Downstream Provider Blocking

The Commission proposes requiring all domestic providers in the call path to block, rather than “simply effectively mitigate,” illegal traffic when notified of such traffic by the Commission, regardless of whether that traffic originates abroad or domestically.²⁸ State AGs support this common-sense requirement. Requiring all domestic providers in the call path to block illegal traffic will provide safeguards to stop or reduce known illegal or fraudulent calling campaigns from reaching consumers, including those who are most vulnerable. State AGs agree with the Commission’s insight that a lack of consistency in blocking obligations for identified illegal robocall traffic across provider types or roles could allow for unintended loopholes that a single, uniform rule would protect against.²⁹ Further, when the Commission has identified illegal traffic, a rule requiring anything short of uniform blocking of that identified illegal traffic would only afford protections to those profiting off of that illegal traffic, and exacerbate the harm those calls can, and will, bring to the nation’s consumers. Thus, because there is no common sense reason to exempt a provider from blocking illegal robocall traffic upon notification to do so by the Commission as described in this Notice, State AGs support the Commission’s proposal to mandate uniform blocking of this illegal traffic.

²⁷ *Id.*

²⁸ *May 2022 FNPRM, supra* note 1, at 70 ¶ 181.

²⁹ *Id.*

C. General Mitigation Standards and the Robocall Mitigation Database

The Commission further proposes extending a general mitigation standard obligation to voice service providers that have implemented STIR/SHAKEN in the IP portions of their networks, and to all domestic intermediate providers.³⁰ This obligation would include a duty for voice service providers to take “reasonable steps” to avoid originating or terminating illegal robocall traffic, and a duty for intermediate providers to take “reasonable steps” to avoid carrying or processing this traffic. Since robocallers and those who enable them often adapt to circumvent specific safeguards targeting illegal traffic,³¹ State AGs agree with the Commission’s proposal to implement a general mitigation obligation for all domestic intermediate providers. This will serve as an “effective backstop” to ensure robocallers “cannot evade any granular requirements” adopted by the Commission.³²

The Commission’s proposed general mitigation standard would also include an obligation for all domestic intermediate providers to file a mitigation plan along with a certification in the Robocall Mitigation Database, which plan must include substantive, detailed practices one could reasonably expect would reduce illegal robocall traffic.³³ State AGs support this proposed requirement, and agree that such an obligation should conform to the obligations that currently apply to gateway providers, namely: (1) certification as to the status of STIR/SHAKEN implementation and robocall mitigation efforts on their networks; (2) contact information for a person responsible for addressing robocall mitigation-related issues; and (3) a detailed description

³⁰ *Id.* at 72 ¶ 188.

³¹ *October 2021 FNPRM*, *supra* note 3, at 32 ¶ 91.

³² *May 2022 FNPRM*, *supra* note 1, at 72 ¶ 188.

³³ *Id.*

of their robocall mitigation practices.³⁴

We further support implementing a requirement that would obligate all domestic providers to “explain what steps they are taking to ensure that the immediate upstream provider is not using their network to transmit illegal calls.”³⁵ Just as STIR/SHAKEN is only truly effective when it is implemented end-to-end, mitigation practices are only effective when providers are accountable and proactive, end-to-end, along the call path. The Commission’s proposal to require providers to be able to “explain” how they are proactively working to mitigate illegal robocall traffic is a reasonable request for any legitimate provider. This obligation should not be overly burdensome for any provider who is committed to consistently keeping illegal traffic off of its network, and State AGs support this proposal.

Moreover, extending these additional mitigation requirements to all domestic providers will also simplify rules for all stakeholders in the robocall ecosystem, subjecting them to the same obligations for all calls, regardless of the providers’ respective roles in the call path.³⁶ Additionally, the application of these requirements industry-wide will enhance the effectiveness of law enforcement efforts pertaining to illegal robocalls.

Finally, State AGs support the shortest compliance deadlines proposed by the Commission for each proposal in this Notice.³⁷ Consumers in our states are eager to see solutions. In fact, they deserve solutions. The sooner the requirements can be implemented industry-wide, the sooner our consumers, and the providers themselves, will benefit from these enhanced protections and guardrails.

³⁴ *Id.* at 75 ¶ 197.

³⁵ *Id.* at 75 ¶ 197.

³⁶ *Id.* at 74 ¶ 193.

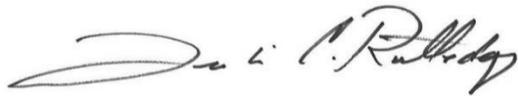
³⁷ *Id.* at 74 ¶ 194.

IV. Conclusion

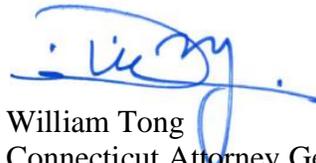
The undersigned State AGs commend the Commission's current proposals to expand obligations to implement Caller ID authentication protocols and specific mitigation efforts to all intermediate domestic providers. Such regulatory symmetry enhances legal clarity and fairness in rule implementation. Imposing consistent obligations on all stakeholders will help law enforcement readily identify and prosecute the bad actors who regularly seek to profit from the illegal robocalls that the nation uniformly abhors.

As with other specific measures adopted in the past, State AGs recognize that the Commission's proposed actions, including mandatory call blocking, will not completely eradicate the illegal robocall epidemic. However, we are confident that the proposals under consideration will help bring bad actors to account. State AGs remain committed to working together, and with the FCC, to combat illegal robocalls, and support the meaningful proposals under consideration by the Commission.

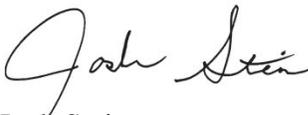
BY FIFTY-ONE (51) STATE ATTORNEYS GENERAL:



Leslie Rutledge
Arkansas Attorney General



William Tong
Connecticut Attorney General



Josh Stein
North Carolina Attorney General



Steve Marshall
Alabama Attorney General



Treg R. Taylor
Alaska Attorney General



Mark Brnovich
Arizona Attorney General



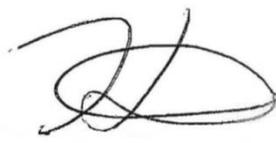
Rob Bonta
California Attorney General



Phil Weiser
Colorado Attorney General



Kathleen Jennings
Delaware Attorney General



Karl Racine
District of Columbia Attorney General



Ashley Moody
Florida Attorney General



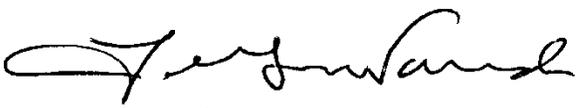
Christopher M. Carr
Georgia Attorney General



Leevin T. Camacho
Guam Attorney General



Holly T. Shikada
Hawaii Attorney General



Lawrence Wasden
Idaho Attorney General



Kwame Raoul
Illinois Attorney General



Todd Rokita
Indiana Attorney General

Tom Miller
Iowa Attorney General

Derek Schmidt
Kansas Attorney General

Daniel Cameron
Kentucky Attorney General

Jeffery Laundry
Louisiana Attorney General

Aaron M. Frey
Maine Attorney General

Brian Frosh
Maryland Attorney General

Maura Healey
Massachusetts Attorney General

Dana Nessel
Michigan Attorney General

Keith Ellison
Minnesota Attorney General

Lynn Fitch
Mississippi Attorney General

Eric S. Schmitt
Missouri Attorney General

Douglas Peterson
Nebraska Attorney General

Aaron D. Ford
Nevada Attorney General

John Formella
New Hampshire Attorney General



Matthew J. Platkin
Acting New Jersey Attorney General



Hector Balderas
New Mexico Attorney General



Letitia James
New York Attorney General



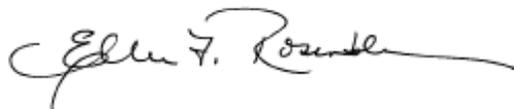
Drew Wrigley
North Dakota Attorney General



Dave Yost
Ohio Attorney General



John M. O'Connor
Oklahoma Attorney General



Ellen Rosenblum
Oregon Attorney General



Josh Shapiro
Pennsylvania Attorney General



Peter F. Neronha
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General



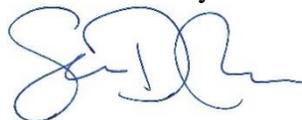
Mark Vargo
South Dakota Attorney General



Jonathan Skrmetti
Tennessee Attorney General



Ken Paxton
Texas Attorney General



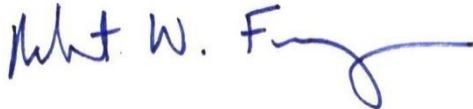
Sean D. Reyes
Utah Attorney General



Susanne Young
Vermont Attorney General



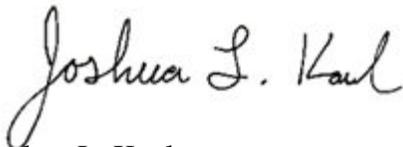
Jason Miyares
Virginia Attorney General



Robert W. Ferguson
Washington Attorney General



Patrick Morrissey
West Virginia Attorney General



Joshua L. Kaul
Wisconsin Attorney General



Bridget Hill
Wyoming Attorney General