



PRESIDENT

Tom Miller
Iowa
Attorney General

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

PRESIDENT-ELECT

Josh Stein
North Carolina
Attorney General

In the Matter of)

Advanced Methods to Target and)
Eliminate Unlawful Robocalls)

CG Docket No. 17-59

VICE PRESIDENT

Ellen F. Rosenblum
Oregon
Attorney General

Call Authentication Trust Anchor)

WC Docket No. 17-97

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

IMMEDIATE PAST
PRESIDENT

Karl A. Racine
District of Columbia
Attorney 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 “take decisive action to stem the tide of foreign-originated illegal robocalls”² by placing “obligations on the gateway providers that are the point of entry for foreign calls into the United States.”³ Consistent with recent submissions to the Commission from

Chris Toth
Executive Director

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

¹ See Fifth Further Notice of Proposed Rulemaking, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, and Fourth Further Notice of Proposed Rulemaking, *Call Authentication Trust Anchor*, WC Docket No. 17-97, Oct. 1, 2021 (“October 2021 FNPRM”).

² *October 2021 FNPRM*, at 1 ¶ 1.

³ *Id.* at 1–2 ¶ 1.

State AGs related to these issues,⁴ we support the Commission’s proposals to require gateway providers⁵ to implement STIR/SHAKEN caller ID authentication in order to verify foreign-originated calls that use U.S.-based phone numbers. Furthermore, and mindful of the continued deluge of illegal foreign-based robocalls that use spoofed, U.S.-based phone numbers, State AGs support the Commission’s proposal to require gateway providers to implement robocall mitigation programs. Gateway providers are liable under the Telemarketing Sales Rule (“TSR”) if they assist and facilitate the making of illegal calls; therefore, they are already obligated to take appropriate steps to monitor the traffic they carry and to take appropriate action to mitigate illegal calls.⁶ Nonetheless, the Commission’s proposal to impose specific and detailed obligations on all gateway providers in a wholistic manner has the potential to reduce illegal traffic on a widespread basis and, thus, merits support.

⁴ See Reply Comments of Fifty-One 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 (“*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).

⁵ For use in these Reply Comments, we adopt the Commission’s proposed definition of “gateway provider” to mean “the first U.S.-based intermediate provider in the call path of a foreign-originated call that transmits the call directly to another intermediate provider or a terminating voice service provider in the United States.” See *October 2021 FNPRM*, at 15 ¶ 33.

⁶ It is a violation of the TSR for any person to provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any practice that violates Sections 310.3(a), (c) or (d), or 310.4 of the TSR. 16 C.F.R. § 310.3(b). Persons who violate this provision of the TSR are said to have “assisted and facilitated” sellers or telemarketers.

Like the Commission, many of our offices report that “unwanted calls, including illegal robocalls, are consistently . . . a top source of consumer complaints.”⁷ Moreover, as the Commission recognizes, illegal robocalls cost law enforcement, the telecommunications industry, and, more importantly, our constituents, approximately \$13.5 billion every year.⁸ In 2020, American consumers, including seniors, persons with disabilities, and other vulnerable populations, were bilked out of \$522 million via fraud perpetrated over the phone and/or through text messages.⁹ In most cases, the perpetrators of this fraud are foreign actors gaining access to the U.S. phone network through international gateway providers.¹⁰ Based upon consumer complaints received by our respective offices, these fraudulent, foreign-originated robocalls often involve caller ID spoofing of U.S.-based phone numbers. In 2021, “caller ID spoofing directed at the United States by [bad actors] operating outside the country” continues to “cause great harm.”¹¹

The time has come to start cutting the strings that form the nets that these illegal robocallers cast over the public. To this end, State AGs encourage the Commission to take this decisive action against illegal, foreign-originated robocalls.

⁷ *Id.* at 2 ¶ 4.

⁸ *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 that are spoofed, to consumers receiving the spoofed calls, and to the terminating carriers who experience increased costs due to consumer complaints).

⁹ *Id.* at 2 ¶ 4.

¹⁰ *Id.* 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.).

¹¹ *Id.* at 2–3 ¶¶ 5, 6 n.8 (recognizing that the IRS continues to warn consumers about phone scams, including IRS impersonation scams, and the Commission continues to warn consumers about auto warranty scams).

II. Call Authentication

Given the “key role gateway providers play in allowing foreign calls into the [U.S.]”,¹² the Commission proposes requiring gateway providers to authenticate foreign-originated calls when the foreign call carries a U.S.-based phone number in the caller ID field.¹³ State AGs support this requirement. As we have previously advocated, universal implementation of STIR/SHAKEN by all voice service providers in the call path is an important step that will provide increased protection for consumers against illegal spoofing.¹⁴

Additionally, the Commission seeks comment on its proposed implementation compliance deadline with respect to a gateway provider’s authentication obligation.¹⁵ State AGs believe that the March 1, 2023 deadline¹⁶ suggested by the Commission is too long for our consumers to wait for enhanced protection from illegally spoofed robocalls. This urgency mirrors that reflected in the Commission’s recent decision to reconsider an initial two-year blanket extension¹⁷ that

¹² *Id.* at 17 ¶ 40.

¹³ *Id.* at 17 ¶ 38.

¹⁴ *August 2021 Reply Comments* 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).

¹⁵ *October 2021 FNPRM*, at 20 ¶ 48.

¹⁶ *Id.*

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* Report and Order and Further Notice of Proposed Rulemaking, *Call Authentication Trust Anchor*, WC Docket No. 17-97, 35 FCC Rcd 3241, 3257–58 ¶¶ 32–35 (2020); 47 CFR § 64.6301. Small voice service providers were granted a two-year extension to June 30, 2023. *See*

expanded the June 30, 2021 STIR/SHAKEN industry-wide implementation deadline, and effectively insulated and enabled a “subset of small voice service providers that are at a heightened risk of originating an especially large amount of robocall traffic.”¹⁸

Because gateway providers are the literal points of entry for illegal and fraudulent foreign robocall traffic using U.S.-based phone numbers to access our U.S. telephone network, a shorter deadline for implementation is necessary. As State AGs advocated in a prior filing with the Commission, gateway providers, especially those that are specifically identified as conduits for illegal robocall traffic, should be required to implement STIR/SHAKEN and begin authenticating call traffic as soon as possible.¹⁹ In addition, we believe the Commission should require the obligation to implement STIR/SHAKEN to become effective within 30 days of the notice of the order being published in the Federal Register.

When it comes to protecting our consumers, the benefits of a shorter deadline outweigh any potential burden to gateway providers. Further, as the Commission recognizes,²⁰ many gateway providers may already be classified as voice service providers and, thus, should have already implemented STIR/SHAKEN into their networks due to their existing obligation to authenticate calls pursuant to the Commission’s rules. Plainly, if a gateway provider is already considered a voice service provider under existing rules, and is not subject to an extension or exemption, such gateway provider should be immediately required to authenticate

Second Report and Order, *Call Authentication Trust Anchor*, WC Docket No. 17-97, 36 FCC Rcd 1859, 1876 ¶ 38 (2020).

¹⁸ See Third Further Notice of Proposed Rulemaking, *Call Authentication Trust Anchor*, WC Docket No. 17-97, May 20, 2021, at 2 ¶ 1.

¹⁹ See *August 2021 Reply Comments*, at 7.

²⁰ *Id.* at 16, 20 ¶¶ 35, 49.

foreign calls that carry U.S.-based phone numbers in the caller ID field. Moreover, gateway providers, in the interest of simply behaving as responsible providers, should already be implementing STIR/SHAKEN.

Lastly, the Commission raises the possibility of granting some gateway providers extensions or exemptions from any obligation that would arise under the proposed rules to authenticate foreign-based call traffic carrying U.S.-based phone numbers in the caller ID field.²¹ However, State AGs urge that strong rules are needed to better protect our consumers from foreign-originated, fraudulent and illegal robocalls, and caller ID spoofing. As such, the Commission's proposed authentication obligation—which is narrowly tailored already—should be imposed without the possibility of extensions or exemptions.

III. Robocall Mitigation

In addition to the requirement of STIR/SHAKEN caller ID authentication, the Commission proposes requiring gateway providers to engage in specific robocall mitigation programs, including: 24-hour traceback response; mandatory call blocking; know-your-customer requirements; adoption of certain contractual provisions with foreign providers; and a general duty to mitigate illegal robocalls.²² By so doing, the Commission proposes that gateway providers employ a dual-pronged approach to foreign-based calls carrying U.S.-based phone numbers—authentication *and* mitigation. State AGs support these proposals, as gateway providers are a vital cog in enabling illegal robocall machinery. Because gateway providers are not sufficiently mitigating illegal traffic, tough rules are necessary.

²¹ *Id.* at 20–21 ¶ 50.

²² *Id.* at 21 ¶ 51.

A. 24-Hour Traceback Requirement

Under the current rules, all domestic voice service providers, including intermediate providers and gateway providers, must respond to traceback requests in a “timely manner.”²³ The Commission proposes requiring that gateway providers 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.²⁴ The Commission further proposes requiring that gateway providers comply with this new obligation within 30 days of notice of the order being published in the Federal Register.²⁵

State AGs support this requirement, as well as the 30-day compliance deadline, because, 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.”²⁶

B. Mandatory Blocking

The Commission is proposing rules that will require voice service providers to engage in mandatory call blocking. State AGs support this requirement. Illegal robocalls, coupled with fraudulent or illegal caller ID spoofing, continue to plague American consumers, and when such

²³ *Id.* (citing 47 CFR § 64.1200(n)(1)); Fourth Report and Order, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, 35 FCC Rcd 15221, 15227–29 ¶¶ 15–21 (2020).

²⁴ *Id.* at 21 ¶ 52.

²⁵ *Id.* at 22 ¶ 55.

²⁶ *Id.* at 21 ¶ 52.

calls originate overseas, enforcement against such bad actors is much more difficult.²⁷ A gateway provider is positioned²⁸ to eradicate—or, at least, significantly mitigate—such fraudulent traffic. If these providers are mandated by the Commission to implement mandatory call blocking, such a directive could help stop an illegal or fraudulent calling campaign before it enters the U.S. telephone network. In turn, U.S. consumers who were the intended targets of such a campaign (oftentimes, senior citizens) will not be victimized, will not have their life-savings depleted and never to be recovered, and will not be made to fear answering their own telephones.

The Commission is proposing several possible approaches, the first of which is to modify an existing rule applicable to all voice service providers.²⁹ Currently, voice service providers, including gateway providers, are required “to take steps to effectively mitigate” illegal traffic when notified by the Commission.³⁰ Gateway providers were put on notice that they may need to block calls in order to comply with this requirement.³¹ Now, the Commission is proposing to “affirmatively require” gateway providers to block calls upon receipt of notification from the Commission’s Enforcement Bureau.³² State AGs support this proposal, and agree with the Commission’s conclusion that it will “better protect American consumers from illegal calls.”³³

²⁷ *Id.* at 22 ¶ 56.

²⁸ *Id.*

²⁹ *Id.* at 22 ¶ 57.

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ *Id.*

To complement mandatory call blocking by gateway providers, the Commission is also proposing to require voice service providers or intermediate providers downstream from the gateway provider to block the calls where the Commission determines that a particular gateway provider is a bad actor.³⁴ Specifically, if a gateway provider should fail to comply with the Commission's proposed authentication and mitigation requirements (for example, the 24-hour traceback request response), the Commission's Enforcement Bureau will be empowered to send a notice to all providers immediately downstream from the gateway provider's call path informing those providers of the gateway's failure to comply.³⁵ Upon receipt of such a notice, all providers will be required to promptly block all traffic from the identified gateway provider, with the exception of 911 and other emergency calls.³⁶

State AGs support this mandatory call blocking proposal, and agree there is significant value in such an approach. Far too often, gateway providers who act as the point of entry for illegal robocalls, coupled with caller ID spoofing of U.S.-based numbers, are entirely non-responsive to traceback requests and government subpoenas. Bad actors who willfully or blindly enable illegal robocalls have no place in the calling ecosystem, and such traffic should be eliminated immediately.

The Commission is also proposing to require gateway providers to block calls that are highly likely to be illegal based on reasonable analytics.³⁷ To aid this effort, the Commission would also require gateway providers to: (1) incorporate caller ID authentication information

³⁴ *Id.* at 23 ¶ 60.

³⁵ *Id.*

³⁶ *Id.* at 23–24 ¶ 60.

³⁷ *Id.* at 25 ¶ 66.

where available; (2) manage blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal, which must include a process that reasonably determines that calling patterns are highly likely to be illegal before initiating blocking; and (3) cease blocking as soon as the provider has actual knowledge the blocked calls are likely lawful.³⁸ State AGs support this call blocking proposal, and agree that it will increase protection for American consumers.

Lastly, the Commission is seeking comment on requiring gateway providers to block calls purporting to originate from numbers that are on a “do-not-originate” list.³⁹ Currently, all voice service providers, including intermediate and gateway providers, are permitted to block calls when the number in the caller ID field is unused, unallocated, or invalid, or where the subscriber to the number has indicated that it does not use the number to originate calls and requests that all calls purporting to originate from that number be blocked.⁴⁰ Consistent with our support of the *First Call Blocking Order*,⁴¹ State AGs encourage the Commission to adopt rules that require gateway providers to block calls from numbers on a do-not-originate list. Since government imposter scams are still plaguing our consumers, this specific mandatory blocking requirement will add another layer of protection.⁴²

³⁸ *Id.*

³⁹ *Id.* at 26 ¶ 71.

⁴⁰ *Id.*; see also Report and Order and Further Notice of Proposed Rulemaking, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, 32 FCC Rcd 9706, 9710–21 ¶¶ 10–40 (2017) (“*First Call Blocking Order*”).

⁴¹ See Comment of 30 State Attorneys General, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket 17-59, filed July 3, 2017.

⁴² With respect to any mandatory blocking rules the Commission enacts, State AGs support the Commission’s proposed compliance deadline of 30 days after publication of the notice of an order in the Federal Register. *October 2021 FNPRM*, at 28–29 ¶ 79.

C. “Know Your Customer” Requirements and Contractual Provisions

The Commission proposes requiring gateway providers, when receiving foreign call traffic in the form of a high volume of calls with a U.S.-based phone number, to confirm that the foreign originator is authorized to use the particular U.S. numbers that are purporting to originate the calls.⁴³ State AGs support this requirement. We agree with the Commission’s assessment that “know your customer” obligations are among the practices that responsible gateway providers should be implementing for all traffic they bring into the U.S. telephone network.⁴⁴ Furthermore, given the sometimes-complex nature of the relationships between originating, intermediate, and gateway providers, State AGs support the Commission’s proposal that gateway providers ensure by contract that their foreign partners validate that the calling party is authorized to use the U.S.-based telephone numbers.⁴⁵

D. General Mitigation Standards and Robocall Mitigation Database

In addition to the specific, proposed requirements above, the Commission is also proposing to require gateway providers to “meet a general obligation to mitigate illegal robocalls,” including submitting a certification to the Robocall Mitigation Database that describes their mitigation practices and avers they are adhering to those practices.⁴⁶ As the Commission recognizes, robocallers can adapt to specific safeguards targeting illegal traffic.⁴⁷ Thus, State AGs support

⁴³ *Id.* at 29 ¶¶ 81, 83.

⁴⁴ *Id.*

⁴⁵ *Id.* at 31 ¶ 88.

⁴⁶ *Id.* at 32–33 ¶¶ 91, 94.

⁴⁷ *Id.* at 32 ¶ 91.

this requirement, and agree that a “general obligation can serve as an effective backstop to ensure that robocallers cannot evade” specific requirements that the Commission adopts.⁴⁸ Moreover, as noted above, gateway providers are already obligated under the law to not assist and facilitate the making of illegal robocalls.

In addition, State AGs support the Commission’s proposed requirement that gateway providers provide a certification to the Robocall Mitigation Database. Furthermore, State AGs support the Commission’s proposed requirement that gateway providers submit the following to the Robocall Mitigation Database: (1) certification as to the status of STIR/SHAKEN implementation and robocall mitigation on their networks; (2) contact information for a person responsible for addressing robocall mitigation-related issues; and (3) a detailed description of their robocall mitigation practices.⁴⁹ Of course, merely providing a certification is not enough. Gateway providers must also actually take the needed action to mitigate illegal robocalls. Simply providing a certification should likewise not be construed as any sort of safe harbor or immunity that reduces or does away with current legal obligations gateway providers currently have under the TSR or elsewhere.

⁴⁸ *Id.*

⁴⁹ *Id.* at 33 ¶ 96.

IV. Conclusion

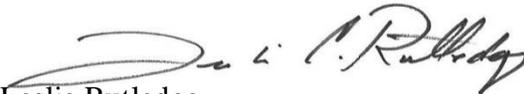
The undersigned State AGs commend the Commission for proposing to take steps designed to deal with foreign-originated, illegal and fraudulent robocalls that purport to be originating from U.S.-based telephone numbers. As with other specific measures adopted in the past, State AGs recognize that the Commission’s proposed actions, including the mandatory call blocking, will not completely solve the illegal robocall and spoofing epidemics. However, more consumers will be protected if these proposals are adopted and effectively implemented. State AGs support these proposals and remain committed to work with the FCC to combat illegal robocalls.

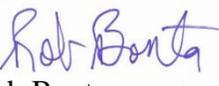
BY FIFTY-ONE (51) STATE ATTORNEYS GENERAL:


Steve Marshall
Alabama Attorney General


Treg R. Taylor
Alaska Attorney General


Mark Brnovich
Arizona Attorney General


Leslie Rutledge
Arkansas Attorney General


Rob Bonta
California Attorney General


Phil Weiser
Colorado Attorney General


William Tong
Connecticut Attorney General


Kathleen Jennings
Delaware Attorney General


Karl A. Racine
District of Columbia Attorney General

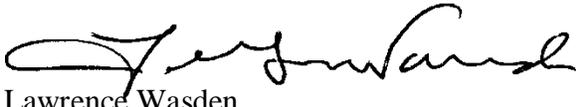

Ashley Moody
Florida Attorney General



Christopher M. Carr
Georgia Attorney General



Holly T. Shikada
Hawaii Attorney General



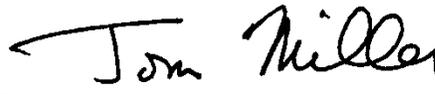
Lawrence Wasden
Idaho Attorney General



Kwame Raoul
Illinois Attorney General



Todd Rokita
Indiana Attorney General



Tom Miller
Iowa Attorney General



Derek Schmidt
Kansas Attorney General



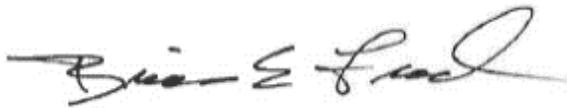
Daniel Cameron
Kentucky Attorney General



Jeff Landry
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



Austin Knudsen
Montana Attorney General



Douglas Peterson
Nebraska Attorney General



Aaron D. Ford
Nevada Attorney General



John M. Formella
New Hampshire Attorney General



Andrew J. Bruck
New Jersey Attorney General



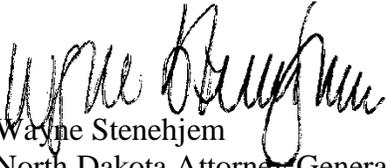
Hector Balderas
New Mexico Attorney General



Letitia James
New York Attorney General



Josh Stein
North Carolina Attorney General



Wayne Stenehjem
North Dakota Attorney General



Dave Yost
Ohio Attorney General



John M. O'Connor
Oklahoma Attorney General



Ellen F. Rosenblum
Oregon Attorney General



Josh Shapiro
Pennsylvania Attorney General



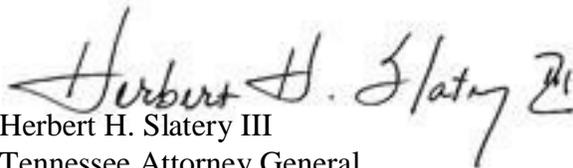
Peter F. Neronha
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General



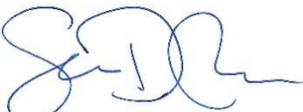
Jason R. Ravensborg
South Dakota Attorney General



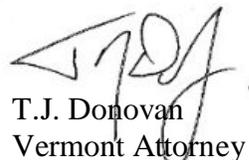
Herbert H. Slatery III
Tennessee Attorney General



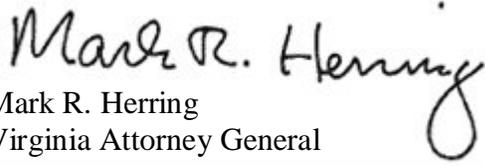
Ken Paxton
Texas Attorney General



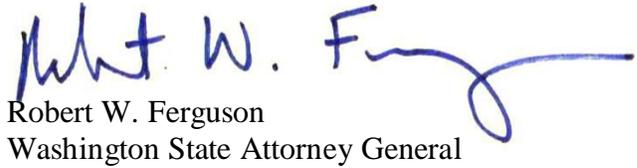
Sean D. Reyes
Utah Attorney General



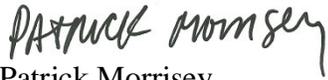
T.J. Donovan
Vermont Attorney General



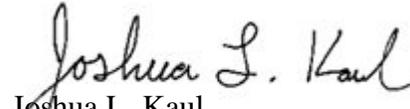
Mark R. Herring
Virginia Attorney General



Robert W. Ferguson
Washington State Attorney General



Patrick Morrissey
West Virginia Attorney General



Joshua L. Kaul
Wisconsin Attorney General



Bridget Hill
Wyoming Attorney General