NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

PRESIDENT
Karl A. Racine
District of Columbia
Attorney General

PRESIDENT-ELECT
Tom Miller
Iowa
Attorney General

VICE PRESIDENT
Josh Stein
North Carolina
Attorney General

IMMEDIATE PAST PRESIDENT
Jeff Landry
Louisiana
Attorney General

Chris Toth
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	)
	)
Numbering Policies for Modern Communications	) WC Dkt No. 13-97
	)
Telephone Number Requirements for IP-Enabled Service Providers	) WC Dkt No. 07-243
	)
	)
Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources	) WC Dkt No. 20-67
	)
	)
	)
Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership	) IB Dkt No. 16-155
	)
	)

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 Wireline Competition and International Bureaus,[1] seeking comment on the Federal Communication Commission's ("Commission") proposals to modify its policies to reduce access to numbers by potential perpetrators of illegal robocalls.

[1] *See* Further Notice of Proposed Rulemaking, *Numbering Policies for Modern Communications*, WC Docket No. 13-97, *et al.*, Aug. 6, 2021 ("*August 2021 Notice*").

Every day, State AGs hear from constituents about the terrible damage inflicted through illegal robocalls. In most State AG offices, illegal robocalls top the list of most frequent consumer complaints. Phone calls and texts are by far the most common contact method for fraud and account for 58% of all fraud with a contact method reported to the Federal Trade Commission—almost four times higher than the next most common contact method.[2] Moreover, fraudulent phone calls and texts account for over $500 million in reported losses.[3]

A scammer's ability to anonymously access numbering resources significantly increases the likelihood that a scammer will be able to successfully defraud consumers. As new technologies such as STIR/SHAKEN call authentication make it more difficult for scammers to remain hidden when they place illegal robocalls, these bad actors will likely increasingly rely on purchasing access to legitimate phone numbers instead of spoofing caller IDs. This is a crucial time to crack down on those who exploit our phone networks to steal personal identifying information and money from consumers. The undersigned State AGs write in support of the Commission's proposals to reduce access to numbering resources by potential perpetrators of illegal robocalls.

II. Anonymous Access to Numbering Resources Undermines STIR/SHAKEN

Caller ID spoofing enables illegal robocalling by allowing scammers and other bad actors to conceal their identities and impersonate legitimate callers. Full end-to-end, industry-wide implementation of STIR/SHAKEN will allow voice service providers to determine which calls are routed using spoofed caller IDs and are likely fraudulent, so that providers can block or label these calls accordingly. However, as state AGs are already seeing, while STIR/SHAKEN is an

[2] Federal Trade Commission, Consumer Sentinel Network Databook 2020, p. 12. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.

[3] *Id.*

important tool to combat illegal robocalls, bad actors are finding other ways to conceal their identities when initiating, originating, and routing high volumes of illegal and fraudulent robocalls.

For instance, purchasing access to phone numbers from companies that do not have meaningful "Know-Your-Customer" policies allows illegal robocallers to circumvent STIR/SHAKEN call authentication. When a robocaller can claim that they have the right to use the calling number—which they can do when they rent or purchase access to phone numbers—their calls will appear to voice service providers as having "full" attestation.[4] Full attestation on rented or purchased numbers acquired by an anonymous robocaller effectively imbues illegal and fraudulent calls with an extra indicia of trustworthiness and, thus, can undermine the effectiveness of call blocking and labeling tools that rely on STIR/SHAKEN call authentication. If a company that provides phone numbers fails to require meaningful identifying information from their subscribers, or blindly accepts unverified and likely false information about a subscriber, then illegal robocallers have the ability to use legitimate phone numbers to place calls with the same degree of anonymity that caller ID spoofing provides.

As the Commission recognizes, "the telecommunications industry has transitioned from a limited number of carriers that all trusted each other to provide accurate calling party origination information to a proliferation of different voice service providers and entities originating calls."[5] Unfortunately, consumers can no longer trust that every company that provides access to phone

[4] *See, e.g.*, Report and Order and Further Notice of Proposed Rulemaking, *Call Authentication Trust Anchor*, WC Docket No. 17-97, Mar. 31, 2020, at ¶ 8 (describing the three different "levels" of attestation as one of the following: "full" or "A" attestation, where the voice service provider indicates by such attestation that it "can confirm the identity of the subscriber making the call, and that the subscriber is using its associated telephone number"; "partial" or "B" attestation, where the voice service provider indicates that it "can confirm the identity of the subscriber but not the telephone number"; or "gateway" or "C" attestation, where the provider indicates only that it "is the point of entry to the IP network for a call that originated elsewhere, such as a call that originated abroad or on a domestic network that is not STIR/SHAKEN-enabled").

[5] *August 2021 Notice* at ¶ 2.

numbers will effectively screen out bad actors. In order to realize STIR/SHAKEN's full potential to reduce illegal robocalls, the Commission must take action to curtail unfettered access to numbering resources by illegal robocallers.

State AGs have been vocal supporters of call blocking and labeling tools, as well as timely implementation of STIR/SHAKEN call authentication. In August 2019, fifty-one State AGs and now-fifteen telecom companies agreed to a set of Anti-Robocall Principles, which included commitments to offer free call blocking and labeling tools to consumers and to implement STIR/SHAKEN call authentication as Principles # 1 and # 2, respectively.[6] More recently, fifty-one State AGs called for faster implementation of STIR/SHAKEN by small voice service providers that flood networks with high volumes of robocalls.[7]

Interconnected VoIP providers with direct access to numbering resources who do not verify their customers' identities, or take steps to ensure that the phone numbers they release into the marketplace are used legally, threaten to undercut the effectiveness of the Anti-Robocall Principles by undermining both STIR/SHAKEN authentication and the improvements to call blocking and labeling tools that STIR/SHAKEN enables. State AGs support the Commission's proposals to require direct access applicants to certify that they will use numbering resources lawfully; not assist and facilitate illegal robocalls, illegal spoofing, or fraud; verify their customers' identities; and take reasonable steps to cut off illegal robocalls transiting their networks once

---

[6] Fifty-One State Attorneys General, *Anti-Robocall Principles*, https://ncdoj.gov/download/141/files/19699/state-ags-providers-antirobocall-principles-feb-2020-with-signatories.

[7] Reply Comments of Fifty-One (51) State Attorneys General, WC Docket No. 17-97 (filed Aug. 9, 2021); *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 August 23, 2019, at 4–6 (supporting 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 implement STIR/SHAKEN).

discovered. These practices will further the goals of the Anti-Robocall Principles by bringing accountability to companies that provide the phone numbers that fuel efforts to circumvent STIR/SHAKEN call authentication.

State AGs also echo the Commission's concern that holders of direct access authorization that supply numbers to new customers on a trial basis are engaging in a practice that "commonly leads to bad actors gaining temporary control over numbers for the purposes of including misleading caller ID information."[8] Providing free, temporary access to phone numbers, as well as through untraceable payment mechanisms, makes it easier for illegal robocallers to hide their identities. Such practices are inconsistent with effective Know-Your-Customer policies.

However, concerns about anonymity and circumventing STIR/SHAKEN and the Anti-Robocall Principles extend not only to those that seek to buy or rent access to legitimate phone numbers in order to initiate or originate illegal and fraudulent robocalls, but also to the VoIP providers themselves that the Commission authorizes to obtain direct access to numbers. Therefore, State AGs support the following proposals and proposed clarifications by the Commission raised in the August 2021 Notice: (1) requiring applicants for direct access to numbers to disclose foreign ownership information; (2) requiring that holders of direct access authorization update the Commission and applicable states within thirty days of any change to the ownership information submitted to the Commission; (3) rejecting an application or revoking an authorization for direct access to numbers of any applicant or holder that has been found to have originated or transmitted illegal robocalls; (4) requiring direct access authorization applicants to certify in the Robocall Mitigation Database that they have fully implemented STIR/SHAKEN or a robocall mitigation program in accordance with certification requirements; (5) requiring that a

[8] *See August 2021 Notice* at ¶ 13.

direct access applicant or authorization holder inform the Commission if it is subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing; and (6) clarifying that interconnected VoIP providers holding a Commission numbering authorization comply with state numbering requirements and other applicable requirements for businesses operating in the state *and* that such must establish minimal state contacts in order to obtain numbering resources in any particular state.[9]

State AGs are confident that these reasonable proposals will help curb illegal robocallers' ability to misuse our nation's limited numbering resources and circumvent the protections of the STIR/SHAKEN call authentication framework. Further, by adopting these proposals, State AGs agree with the Commission that such clarifications and guardrails would "better ensure that VoIP providers that obtain the benefit of direct access to numbers comply with existing legal obligations and do not facilitate illegal robocalls[.]"[10]

III. Restraining the Misuse of Numbering Resources Before Enlarging Access to Such Resources

Many of the most pernicious scams rely on call-back numbers to maintain contact with the victim. If a robocaller blocks or spoofs their calling number, they are unable to interact with potential victims after the initial robocall. Thus, recent enforcement actions show that some interconnected VoIP companies cater to the needs of robocallers by providing *both* call termination services *and* access to call-back numbers to act as a one-stop-shop for running illegal robocall campaigns.[11] However, these bad actor VoIP providers who court customers engaged in

[9] *See id.* ¶¶ 11, 14, 15, 23–25, 30, 33, 36, and 37.

[10] *See id.* ¶ 3.

[11] *See United States v. Palumbo*, 448 F. Supp. 3d 257, 264 (E.D.N.Y. 2020) (enjoining VoIP provider that transmitted fraudulent robocalls and sold access to phone numbers which it obtained indirectly from another VoIP provider and concluding: "Defendants' business of selling call-back (such as direct-inward-dial) numbers to clients is also a key element of the fraud. The call-back

illegal robocalling are only a part of the problem because robocallers purchase call-back numbers from a variety of sources, including through phone number resellers who provide inbound service, either directly or through apps.

Nevertheless, whether they acquire access to phone numbers through interconnected VoIP providers with direct access to numbering resources, or on the secondary market through phone number resellers, illegal robocallers' primary objective is hiding their identity in order to perpetrate scams against consumers. Robocallers will seek out companies that provide phone numbers without conducting proper due diligence in order to thwart efforts to hold them accountable for the destructive consequences of their calls.

Moreover, because the need to constrain the rampant misuse of legitimate numbers must be a priority, State AGs urge the Commission to refrain from expanding its authorization process for direct access to numbers to one-way VoIP providers or other entities that use numbers until such time that the guardrails identified in the August 2021 Notice can be ordered, implemented, and effectively deployed in order to shore up the current process consistent with the proposals identified by the Commission.

The Commission's proposals requiring direct access applicants to certify that they know their customer through customer identity verification and that they will not encourage or assist and facilitate illegal robocalls, spoofing, or fraud are important steps to combat the epidemic of robocalls. However, to better address this problem, a broader approach is necessary. *Any company* that provides access to phone numbers without accurately and fully verifying the identity of their customer is assisting and facilitating all illegal robocalls that utilize that phone number, either for placing the robocalls or as a call-back number. State AG's applaud the Commission's proposals

---

numbers provide a seamless way for the robocall victim-recipients to return calls . . . in practice, this connects them with human fraudsters who . . . seek to part them from their savings.").

to address illegal robocallers by leveraging access to numbering resources as highlighted herein, and urge the Commission to pursue further regulatory and legislative action to address this important issue.

IV. Conclusion

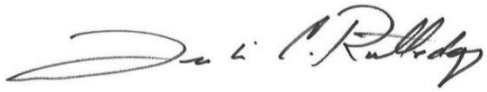
Together, State and Federal authorities are making progress in curtailing illegal robocalls; however, much work remains to be done. State AGs are pleased to support the Commission's efforts to restrict access to numbering resources by illegal robocallers and urge further and aggressive action by the Commission to restrict robocallers' ability to shield their identities and exploit consumers' trust in our telephone system.

BY FIFTY-ONE (51) STATE ATTORNEYS GENERAL:

Steve Marshall
Alabama Attorney General

Treg R. Taylor
Alaska Attorney General

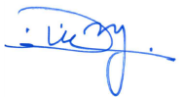
Mark Brnovich
Arizona Attorney General



Leslie Rutledge
Arkansas Attorney General

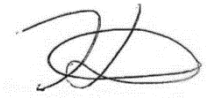
Rob Bonta
California Attorney General

Phil Weiser
Colorado Attorney General



William Tong
Connecticut Attorney General

Kathleen Jennings
Delaware Attorney General

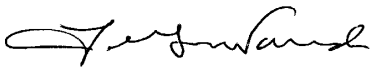


Karl A. Racine
District of Columbia Attorney General

Ashley Moody
Florida Attorney General

Christopher M. Carr
Georgia Attorney General

Clare E. Connors
Hawaii Attorney General



Lawrence Wasden
Idaho Attorney General

Kwame Raoul
Illinois Attorney General

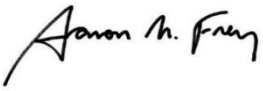
Todd Rokita
Indiana Attorney General

Tom Miller
Iowa Attorney General

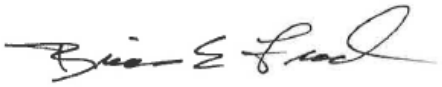
Derek Schmidt
Kansas Attorney General

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 Acting Attorney General

Hector Balderas
New Mexico Attorney General

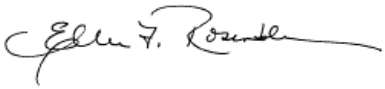
Letitia James
New York Attorney General

Joshua H. Stein
North Carolina Attorney General

Wayne Stenehjem
North Dakota Attorney General

Dave Yost
Ohio Attorney General

John M. O'Connor
Oklahoma Attorney General



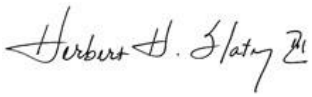
Ellen F. Rosenblum
Oregon Attorney General

Josh Shapiro
Pennsylvania Attorney General

Peter F. Neronha
Rhode Island Attorney General

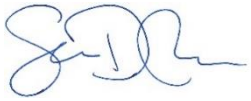
Alan Wilson
South Carolina Attorney General

Jason R. Ravnsborg
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 Morrisey
West Virginia Attorney General

Joshua L. Kaul
Wisconsin Attorney General

Bridget Hill
Wyoming Attorney General