

## **ANTI-ROBOCALL PRINCIPLES**

State Attorneys General and the undersigned voice service providers are committed to stopping illegal and unwanted robocalls for the American people. Therefore, state Attorneys General have engaged voice service providers to gain their support and assistance in combatting this pervasive problem. These Anti-Robocall Principles are the product of this engagement.

Illegal and unwanted robocalls continue to harm and hassle people every day. Consumer fraud often originates with an illegal call, and robocalls regularly interrupt our daily lives. Robocalls and telemarketing calls are the number one source of consumer complaints at many state Attorneys General offices, as well as at both the Federal Communications Commission and the Federal Trade Commission. State Attorneys General are on the front lines of enforcing do-not-call laws and helping people who are scammed and harassed by these calls.

Through law enforcement and technological developments, respectively, state Attorneys General and voice service providers are working to assist consumers and battle bad actors who scam consumers and intrude upon their lives. By implementing call blocking technology, knowing their customers, actively monitoring their networks for robocall traffic, cooperating in investigations that trace the origins of illegal robocalls, and integrating other practices enumerated in the Anti-Robocall Principles, these voice service providers will aid the state Attorneys General in identifying and prosecuting illegal robocallers.

## ANTI-ROBOCALL PRINCIPLES FOR VOICE SERVICE PROVIDERS

**The undersigned voice service providers declare that they will work with the undersigned state Attorneys General by incorporating, or continuing to incorporate, these Anti-Robocall Principles into their business practices:**

**Principle #1. Offer Free Call Blocking and Labeling.** For smartphone mobile and VoIP residential customers, make available free, easy-to-use call blocking and labeling tools and regularly engage in easily understandable outreach efforts to notify them about these tools. For all types of customers, implement network-level call blocking at no charge. Use best efforts to ensure that all tools offered safeguard customers' personal, proprietary, and location information.

**Principle #2. Implement STIR/SHAKEN.** Implement STIR/SHAKEN call authentication.

**Principle #3. Analyze and Monitor Network Traffic.** Analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls.

**Principle #4. Investigate Suspicious Calls and Calling Patterns.** If a provider detects a pattern consistent with illegal robocalls, or if a provider otherwise has reason to suspect illegal robocalling or spoofing is taking place over its network, seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name, terminating the party's ability to originate, route, or terminate calls on its network, and notifying law enforcement authorities.

**Principle #5. Confirm the Identity of Commercial Customers.** Confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.

**Principle #6. Require Traceback Cooperation in Contracts.** For all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.

**Principle #7. Cooperate in Traceback Investigations.** To allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom's Industry Traceback Group. Identify a single point of contact in charge of responding to these traceback requests, and respond to traceback requests as soon as possible.

**Principle #8. Communicate with State Attorneys General.** Communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling. Due to the ever-changing nature of technology, update the state Attorneys General about potential additional solutions for combatting illegal robocalls.

## DEFINITIONS OF TERMS IN ANTI-ROBOCALL PRINCIPLES

The following terms are used in the attached set of Principles:

- **CALL AUTHENTICATION:** Call authentication allows a voice service provider to cryptographically sign call signaling information and allows the intermediate and destination providers to validate the signature. Call authentication prevents a caller from disguising its true identity and/or call origination. Call authentication is provided by a set of standards called STIR/SHAKEN, which specifies this functionality for Voice over Internet Protocol (“VoIP”) calls.
- **CALL BLOCKING:** Call blocking consists of technologies or devices that can stop illegal robocalls before they reach the called party. Call blocking can be implemented by various means on a voice service provider’s network or can be activated by the consumer through software applications or other devices or services.
- **CALL BLOCKING TOOLS:** Call blocking tools are devices, software applications, or services that may be pre-installed, downloaded, enabled, or manually programmed for individual use by consumers. Call blocking tools may be offered directly by the provider or made available through third parties.
- **CALL LABELING:** Call labeling passes additional information about an incoming call to the called party beyond the caller’s telephone number and caller ID name. It is typically displayed on the landline caller ID display or the mobile device screen. The information may display something like “spam” or “fraud alert” in text, or it may suggest the likelihood of an unwanted call by color, score, or image. The information may be provided by the voice service provider or by third-party software and services.
- **NETWORK-LEVEL CALL BLOCKING:** Network-level call blocking by the voice service provider stops calls from reaching a consumer’s landline or cellular telephone device without the consumer taking any steps to activate, request, opt-in, opt-out, or enable the blocking.
- **SHAKEN:** Signature-based Handling of Asserted information using toKENs. SHAKEN is an industry standard that defines how voice service providers should implement the STIR technology to ensure that outbound or originating calling party numbers are not illegally spoofed.
- **STIR:** Secure Telephony Identify Revisited. STIR is the name of a standardization working group and is commonly used to label the technology that adds cryptographic signatures to call signaling requests. This technology prevents a caller from providing a calling number to the receiving party that the caller is not authorized to use.

## DEFINITIONS OF TERMS (*continued*)

- **STIR/SHAKEN:** STIR/SHAKEN describes a set of technical standards and operating procedures for implementing call authentication for calls carried over an Internet Protocol network. The STIR/SHAKEN framework will enable originating voice service providers to attest to the validity of asserted caller IDs and sign outbound calls with a secure signature or certificate that cannot be faked. The terminating service provider will use the security certificate to validate that the caller ID attestation has not been compromised.
- **TRACEBACK:** Traceback is the process of determining the origin of a call, typically by starting with the receiving party and terminating voice service provider and tracing backwards through the path of the intermediate providers and, ultimately, to the originating voice service provider and the origin of the call. Traceback can be used to find the source of robocalls and, thus, the entities responsible for those calls.
- **VoIP:** Voice over Internet Protocol. VoIP carries voice telephone calls over Internet Protocol networks, either within and between voice service providers or to the end customer.

## DISCLAIMER

Failure to adhere to these principles is not in itself a basis for liability nor does adherence to these principles protect or release any party from liability. Compliance with these principles does not relieve any party from its duty to comply with state or federal laws and regulations. Adherence to these principles may take time for the voice service providers to plan for and implement.

AGREED to and SUPPORTED by the undersigned state Attorneys General and voice service providers:

AT&T Services, Inc.

Bandwidth Inc.

CenturyLink

Charter Communications, Inc.

Comcast

Consolidated Communications, Inc.

Frontier Communications Corporation

Sprint

T-Mobile USA

U.S. Cellular

Verizon

Windstream Services, LLC

JOSHUA H. STEIN  
Attorney General  
State of North Carolina

GORDON J. MACDONALD  
Attorney General  
State of New Hampshire

CURTIS T. HILL, JR.  
Attorney General  
State of Indiana

STEVE MARSHALL  
Attorney General  
State of Alabama

KEVIN G. CLARKSON  
Attorney General  
State of Alaska

MARK BRNOVICH  
Attorney General  
State of Arizona

LESLIE RUTLEDGE  
Attorney General  
State of Arkansas

XAVIER BECERRA  
Attorney General  
State of California

PHIL WEISER  
Attorney General  
State of Colorado

WILLIAM TONG  
Attorney General  
State of Connecticut

KATHLEEN JENNINGS  
Attorney General  
State of Delaware

KARL A. RACINE  
Attorney General  
District of Columbia

ASHLEY MOODY  
Attorney General  
State of Florida

CHRISTOPHER M. CARR  
Attorney General  
State of Georgia

CLARE E. CONNORS  
Attorney General  
State of Hawaii

LAWRENCE G. WASDEN  
Attorney General  
State of Idaho

KWAME RAOUL  
Attorney General  
State of Illinois

TOM MILLER  
Attorney General  
State of Iowa

DEREK SCHMIDT  
Attorney General  
State of Kansas

ANDY BESHEAR  
Attorney General  
Commonwealth of Kentucky

JEFF LANDRY  
Attorney General  
State of Louisiana

AARON M. FREY  
Attorney General  
State of Maine

BRIAN E. FROSH  
Attorney General  
State of Maryland

MAURA HEALEY  
Attorney General  
Commonwealth of Massachusetts

DANA NESSEL  
Attorney General  
State of Michigan

KEITH ELLISON  
Attorney General  
State of Minnesota

JIM HOOD  
Attorney General  
State of Mississippi

ERIC S. SCHMITT  
Attorney General  
State of Missouri

TIM FOX  
Attorney General  
State of Montana

DOUGLAS PETERSON  
Attorney General  
State of Nebraska

AARON D. FORD  
Attorney General  
State of Nevada

GURBIR S. GREWAL  
Attorney General  
State of New Jersey

HECTOR BALDERAS  
Attorney General  
State of New Mexico

LETITIA A. JAMES  
Attorney General  
State of New York

WAYNE STENEHJEM  
Attorney General  
State of North Dakota

DAVE YOST  
Attorney General  
State of Ohio

MIKE HUNTER  
Attorney General  
State of Oklahoma

ELLEN F. ROSENBLUM  
Attorney General  
State of Oregon

JOSH SHAPIRO  
Attorney General  
Commonwealth of Pennsylvania

PETER F. NERONHA  
Attorney General  
State of Rhode Island

ALAN WILSON  
Attorney General  
State of South Carolina

JASON R. RAVNSBORG  
Attorney General  
State of South Dakota

HERBERT H. SLATERY III  
Attorney General  
State of Tennessee

KEN PAXTON  
Attorney General  
State of Texas

SEAN D. REYES  
Attorney General  
State of Utah

T.J. DONOVAN  
Attorney General  
State of Vermont

MARK R. HERRING  
Attorney General  
Commonwealth of Virginia

ROBERT W. FERGUSON  
Attorney General  
State of Washington

PATRICK MORRISEY  
Attorney General  
State of West Virginia

JOSHUA L. KAUL  
Attorney General  
State of Wisconsin

BRIDGET HILL  
Attorney General  
State of Wyoming