



Robocall Mitigation Plan for Bandwidth Inc. and Its Affiliated Providers

Bandwidth Inc. (Bandwidth) has been a long-standing active participant and leader in the key industry organizations and efforts to stop illegal robocalling. Bandwidth was one of the major carriers invited by Chairman Wheeler to create the original Robocall Task Force¹ and ever since has been at the forefront of industry efforts to restore trust into an ever-evolving communications ecosystem. Bandwidth believes that all consumers will benefit to the greatest degree when carriers and service providers can accurately identify illegal robocalls while simultaneously ensuring that valid communications are not improperly affected. Ensuring that the prevention of illegal robocall coexists with effective traffic delivery of legal calls across the global communications ecosystem will depend critically upon the effective use of multi-faceted tools like the RMD together with other industry best practices² and the increased adoption of SHAKEN/STIR specifications.

By leveraging its all-IP network capabilities, Bandwidth has been well positioned as an industry leader for the implementation of the STIR/SHAKEN framework. Further, Bandwidth was among the founding members of the Industry Traceback Group (ITG) and continues to be an active participant and Executive Committee member. Among a number of other leadership roles and responsibilities, Bandwidth is a long-standing member of the North American Numbering Council (NANC) and has been a supporter of the NANC's CATA Working Group as well as the NAOWG and their work establishing the industry's STIR/SHAKEN framework³ and the Commission's Reassigned Numbers Database (RND).

A large majority of Bandwidth's traffic and services are supported in its capacity as an Intermediate Service Provider without direct end-user relationships. In a similar role, Bandwidth may also from time to time operate in the role of an International Gateway Provider, albeit at considerably smaller volumes than its domestic Intermediate provider capacity. Bandwidth also operates as a Voice Service Provider with its relatively small but growing retail enterprise focused business where it may directly enable and support direct-to-consumer services. Bandwidth's fraud operations manage all of these combined roles and responsibilities collectively but with a clear understanding of the differences that require different operational systems, tools and supporting process and procedure. For example, Bandwidth's VSP enterprise focused services include the ability to incorporate a variety of tools to ensure robust consumer protections are in place, such as voice recognition, real-time "robo-scoring", opt-in or opt-out among others that are designed to help avoid the delivery and receipt of illegal robocalls. While more generally, Bandwidth also actively supports research efforts that are specifically designed to help develop robocalling data and solutions for call authentication and analytics to stop the transmission of illegal robocalling on

¹ <https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf>

² See State Attorneys General Anti-Robocalling Principles:
<https://oag.ca.gov/system/files/attachments/press-docs/State%20AGs%20Providers%20AntiRobocall%20Principles-With%20Signatories.pdf>

³ See: <https://sti-ga.atis.org/leadership/>

its network and for the industry collectively.⁴ Across all of its service provider roles Bandwidth continues to have fraud mitigation success with its three-pronged operational approach (prevent, detect, and mitigate) that incorporate FCC mandates and industry best practices for each of its roles as described more fully below.

TECHNICAL AND OPERATIONAL FOUNDATIONS OF BANDWIDTH’S PLAN FOR ALL OF ITS DISCRETE SERVICE PROVIDER ROLES

Bandwidth’s Robocall Mitigation Plan is premised upon a three-pronged set of technical and operational procedures, the details of which can be summarized as follows:

1) Prevention:

- a. **Customer Onboarding.** Bandwidth has a stringent on-boarding screening process designed to proactively identify and prevent those that may engage in illegal robocalling from becoming Bandwidth customers at the outset. On-boarding screening procedures will always take Bandwidth’s specific service provider role into account but the fundamentals of its on-boarding review procedures apply to all of Bandwidth’s Intermediate, International Gateway and VSP services alike and we consider them to be the core of our “Know Your Customer” practices, which also inherently include “Know Your Upstream Provider” now in the context of the Commission’s updated rules and terminology in wholesale service model scenarios (collectively “KYC”). Bandwidth tracks and records government enforcement actions and ever evolving industry trends to have up-to-date information on problematic use cases and known bad actors. Accordingly, Bandwidth requires that all of its upstream service providers (who may themselves be “Intermediate Providers”, “Gateway Providers”, “Originating Voice Service Providers” or “Foreign Service Providers”) customers maintain valid registrations in the FCC’s Robocall Mitigation Database (“RMD”) and requires clear service-specific contractual requirements in which customers agree to cooperate with the ITG and agree to follow all applicable laws against illegal robocalling, fraud and abuse.
- b. **Existing Customer Review.** After our initial “KYC” on-boarding screening, Bandwidth’s operations personnel stay closely aligned with its customers and the industry’s anti-robocalling efforts and developments to remind, educate and clarify what behaviors may signal or constitute unlawful robocalling, and continually notify customers when we identify instances that need their attention in order to prevent illegal robocalling behaviors on their networks. In 2025, Bandwidth went through an effort to update its attestation policies and

⁴ See, e.g., (North Carolina State Robocall Study) <https://news.ncsu.edu/2020/08/study-debunks-robocall-myths/>

practices for all of its reseller customers where Bandwidth typically operates as a non-Gateway Intermediate Provider as well as where it may serve as an Intermediate Gateway provider at times as well. Bandwidth notified potentially impacted existing customers of this change in detail and in writing on May 20, 2025. Bandwidth also established a new robust set of internal processes by which operations personnel engaged in an extensive KYC refreshed review of existing customers and their services. In this updated review, Bandwidth has collected a multitude of data points from and about its customers, including but not limited to, use case descriptions and call flow diagrams. Bandwidth then analyzed and determined what it deemed to be the appropriate attestation levels for unsigned calls received from that customer in accordance with ATIS and FCC rules and objectives. The ultimate goal of Bandwidth's practices is to work to enable originating caller transparency on an end-to-end basis as Bandwidth and the broader industry continue their mitigation efforts against illegal robocalling, fraud, and abuse.

- 2) **Monitoring and Detection:** Bandwidth has a team of operational experts who have implemented technical and operational processes and procedures to monitor, detect and analyze the use of its services and traffic on our network that helps to determine when illegal and inappropriate robocalling activity may be occurring. Bandwidth has developed and deployed a "Call Blocking Tool" that incorporates industry best practices into its core network to identify and block invalid, unallocated and otherwise obviously illegal telephone numbers. Further, even though it acts predominantly as an "Intermediate Provider", Bandwidth implemented STIR/SHAKEN in its all-IP core network infrastructure long before it was mandated by the FCC and has been working to increase call detail transparency and collaborative traceback enablement for years. When unlawful robocall campaigns are detected, Bandwidth follows established processes and procedures to notify upstream customers of the problematic traffic and request that they take immediate corrective actions to prevent reoccurrence of the illegal calls. Bandwidth's engagement and support for the ITG Tracebacks also includes work to monitor that its upstream providers are effectively cooperating with the ITG and working to address the sources of each traceback event. Bandwidth consistently analyzes its call detail records to identify problematic call patterns and their sources from where it sits in a myriad of traffic flows. Bandwidth then incorporates these learnings into its traffic data analytics and detection technologies to continually improve its capabilities to accurately detect suspected illegal activity and deploy mitigation measures.
- 3) **Mitigation:** Bandwidth's operations personnel are positioned to rapidly assist the ITG with the industry's collective efforts to identify the originating sources of illegal activities on the PSTN and prevent further delivery of unwanted and illegal traffic to the greatest degree possible. Bandwidth tracks its ITG request data and conducts considerable outreach to upstream customers that have sent traceback traffic to Bandwidth. Bandwidth's upstream provider mitigation efforts aim to achieve demonstrable improvements in call quality, while also accounting for call quantities

that are being serviced as well. When necessary and appropriate, Bandwidth can formally demand customers be put on a performance improvement plan, or if past mitigation efforts have failed, Bandwidth does take corrective action to terminate service arrangements that place Bandwidth and downstream providers and consumers at risk. Bandwidth's commitment to the benefits of STIR/SHAKEN in an all-IP network environment advances improvements in accurate and targeted call blocking that are designed to block calls from invalid and illegal telephone numbers in keeping with industry best practices and the FCC's recommendations, while simultaneously work to prevent anti-competitive and discriminatory blocking and mislabeling that is unfortunately plaguing the competitive industry with overly broad and blunt analytics. Bandwidth also works closely with Law Enforcement Agencies (LEA) at all levels of government and with its interconnected carrier partners. Bandwidth's fraud and security experts are constantly working to respond to complaints and trouble tickets with customers that may be associated with the unlawful uses of Bandwidth's services. In addition to these notifications, we then aim to work diligently together with our customers and other industry members to stop the unlawful robocall campaigns being detected. Finally, together with its active involvement in the ITG, Bandwidth supports the industry's established Do Not Originate (DNO) efforts pursuant to the industry best practices and procedures.

AFFILIATED ENTITIES COVERED BY BANDWIDTH'S ROBOCALLING MITIGATION PLAN:

Bandwidth is the sole owner and operator of its underlying competitive local exchange carrier Bandwidth.com CLEC, LLC, which is managed together and in accordance with this Robocall Mitigation Plan. Further, in November 2020 Bandwidth acquired Voxbone S.A. and while Bandwidth continues to work to fully integrate all of its operational capabilities with those of Voxbone, the Voxbone entities are also subject to the robocall mitigation policies and procedures described in this document. Therefore, the following entities are also explicitly incorporated into Bandwidth's plan:

- Bandwidth.com CLEC, LLC
- Voxbone S.A.