



CALLTOWER, INC. ROBOCALL MITIGATION PLAN

I. BACKGROUND

Under the authority Congress granted the Federal Communications Commission (“FCC” or “Commission”) in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Commission has adopted rules requiring voice service providers, like Calltower, Inc (“The Company”), to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks. 47 CFR § 64.6301, Secure an IPES OCN, require Carriers to procure tokens.

The FCC requires that all voice service providers certify and upload a copy of a Carriers most recent and up to date Robocall Mitigation Plan (as specified in the FCC’s 6th Order) by February 26, 2024. A Carrier is required to take such steps in the Commission’s [Robocall Mitigation Database](#); whether they have implemented STIR/SHAKEN and that a Carrier has documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on a Carriers network.

The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

The Company is dedicated to stopping illegal calls from originating on its network and undertaking commercially reasonable efforts to monitor the calls coming into its network, consistent with FCC regulations and its “Best Practices” guidance.

This document outlines the Company’s Robocall Mitigation Plan.

II. COMPANY INFORMATION

Company Background and Description

Since its inception in 2002, The Company has evolved into a global cloud-based, enterprise-class Unified Communications, Contact Center and Collaboration solutions provider for growing organizations worldwide.

The Company provides, integrates and supports industry-leading solutions, including Operator Connect for Microsoft® Teams, Teams Direct Routing, GCC High Teams Direct Routing, Office 365, Cisco® Webex Calling / UCM, Cisco® CCPP, Zoom (BYOC), Zoom Phone, CT Cloud UCaaS and four contact center options, including Five9 for business customers.

The Company is at the forefront of the industry by being first to market, with unique Products and Services to always meet the critical needs of its existing clients and acquiring new ones rapidly by deploying best-in-class Services.

a. IPES OCN

The Company IPES OCN is: **630J**.



b. The Company Main Address & Contact Information

10701 S River Front Pkwy,
South Jordan, UT 84095
Toll Free: (800) 347-5444
Company Web Site: www.calltower.com

c. FRN and 499 Filer ID Numbers

Company FRN/CORES ID: 0006745434
Company 499Filer ID: 823246

d. Officers and Directors

CEO and President

Name: Bret L England

10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095

Direct Dial Phone: 1-801-934-3736

Email: bengland@calltower.com

CFO and Secretary

Name: Shawn Hansen

10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095

Direct Dial Phone: 1-385-259-6210

Email: shansen@calltower.com

CTO

Name: Brandon Watts

10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095

Direct Dial Phone: 1-801-702-4249

Email: bwatts@calltower.com

Regulatory Contact:

Name: Shawn Hansen

10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095

Direct Dial Phone: 1-385-259-6210

Email: compliance@calltower.com

RMD/STIR/SHAKEN Contact:

Name: Brandon Watts

10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095

Direct Dial Phone: 1-801-702-4249

Email: regcompliance@calltower.com

e. Nature of the Company “In the Call Flow”

As noted above, presently the Company provides its services to direct end user business and enterprise customers. The Company has its own switch and sound relationships with Transnexus and its underlying upstream carriers such as Bandwidth, Lumen and Verizon.



originate and terminate traffic on its own network. The Company is capable of authenticating the calling party's relationship with the caller ID ascribed to a given call. The Company's network is, also more than capable of accepting and accurately transmitting all STIR/SHAKEN-related data it receives in the call path. And for outbound calls from known customer telephone numbers that originate on our network, The Company will sign calls with the STIR/SHAKEN parameters and mandates as defined in FCC orders.

f. Affiliated Companies:

1. By Acquisition:
 1. Broadriver Communications Corporation
 2. Appia Communications, Inc.
 3. Onestream Networks, LLC

The Company has acquired multiple companies since 2018. These companies were integrated into The Company's systems, network, and processes.

g. Holding Companies:

1. BV Calltower Topco, Inc.
2. BV Calltower Buyer, Inc.
3. Calltower Holdings, Inc.

The Company is owned by a chain of holding companies. Calltower Holdings, Inc. was formed in 2018 and BV Calltower Topco, Inc. and BV Calltower Buyer, Inc. were formed in 2023.

III. COMPANY Know Your Customer ("KYC") Standards

As part of its customer-onboarding process, the Company undertakes very stringent and various commercially reasonable precautions to verify a given customer's identity, including having its customers complete:

- a. Intake and Onboarding Documents
- b. A formal written contract/Master Service Agreement
- c. Service Orders
- d. Company FEIN Number

Among other data points collected and, as appropriate, verified, as part of those processes the Company may also gather the following customer-identifying facts and circumstances:

- a. Customer business name,
- b. Business/Trade and bank references,
- c. Physical business location,
- d. Credit Application,
- e. Contact person(s) at times more detailed information, and
- f. Federal tax identification number

The Company also uses best and reasonable efforts to confirm the identity of new commercial voice customers by collecting information such as physical business location, contact person(s), federal tax identification, and understanding the nature of the customer's business including if/how they will employ auto-dialers or other robocall style tools in the conduct of their business.



At this point in time the Company does not resell its VoIP services to other resellers and only sells service to business customers and business enterprises, the Company still seeks to meet all requirements when validating its customers calls.

If and when and in the future the Company changes its business model to support other Carriers as resellers of the Company products and Services, the Company will require significant information related to that reseller.

If and when in the future the Company resells its Services to reseller Carriers along with requisite FUSF exemption forms, additional Exemption forms when and where appropriate will also be provided to the reseller for Completion along with a very detailed KYC Form.

The KYC form will request that the reseller will provide information without limitation to include FRM/CORES ID, 499 Filer ID and questions will include the Customer to provide information relative to in the Customer has ever received:

- a. FCC NAL within the last 5 years;
- b. A notice or communications stating that they have violated any rules, guidelines and parameters within the TCPA and/or been cited by any state or Federal government for Robocalling;
- c. Any citations from the FTC and/or any PUC or PSC for suspected or actual telemarketing violations
- d. What practices does the reseller carrier employ related to STIR/SHAKEN, Robocall Mitigation and other FCC regulations;
- e. Has the reseller customer ever been terminated or had its relationship terminated with any carriers in the last 3 years for any reason (if so please explain); and,
- f. Additional questions to establish that the reseller is a strong company that employs all standards and policies of Federal and state regulation and has never been accused of being a “bad actor” or contributing to the industry in a negative way.

As applicable, if and when the Company provides Service to resellers; the Company’s verification practices will also include confirming a customer’s reported status in the FCC’s Form 499 Filer database of registered carriers, and, as of February 26, 2024, the Commission’s Robocall Mitigation Database.

The Company also conducts, as applicable, credit checks and checks references with a prospective customer’s bank and trade references as part of its internal financial and contract processes.

IV. COMPANY’S Acceptable Use Policy

As part of its customer-onboarding process and the Company Terms and Conditions, all of the Company’s customers agree to various terms and conditions by execution of a formal Agreement to support the business relationship. These documents (Terms and Conditions, MSA, Privacy Policy, Opt-In/Out Policy) also include and require them to sign their acceptance and agreement to be in compliance with the Company’s Acceptable Use Policy (AUP). Without limitation the Company AUP prohibits:

- a) Using the Services to engage in any activities that are illegal, abusive, false,



fraudulent, deceptive, or misleading, or any activity that exploits, harms, or threatens to harm children, human trafficking and/or any other like or similar unlawful activity.

b) Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including, without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.

c) Using the Company's Services in any way that fails to comply and conform with any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.

d) Creating a false or misleading identity, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

All requisite Company legal documents with its customers stipulate that the Company has immediate authorization to suspend and/or terminate all Services in the event of an AUP violation (and/or any other material term to any documents incorporated by reference to that AUP policy) effective immediately.

V. PROACTIVE NETWORK MONITORING

The Company has various monitoring and reporting systems in place to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls and/or other potentially unlawful usage.

For example, the Company's monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, without limitation:

- a. Blocking calls for which the caller ID is not part of a valid, in-use number range.
- b. Using monitoring systems to alert CallTower personnel for investigation on high levels of short duration calls or low call completion percentage.

If the Company detects any pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling, spoofing or any form of fraud is occurring on its network, the Company takes immediate action to identify the party that is using its network to carry these calls and takes appropriate action to halt, suspend and/or terminate the calls and also if and when applicable the Customer.

VI. TRACEBACK REQUESTS & INVESTIGATING SUSPICIOUS ACTIVITY

The company firmly commits to timely cooperating with and responding to Traceback requests from the ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas and other valid legal processes.



As defined in more detail below the Company has dedicated ample resources to provide prompt and complete responses to such requests. The Company always investigates suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.

When The Company supports reseller Customers, The Company will comply with all parameters of the Industry Traceback Group (“ITG”) and will actively work with ITG’s recommended best industry practices and cooperates with all ITG traceback investigations. To allow for prompt and comprehensive responses, the Company will allocate dedicated resources to provide quick and complete responses to traceback requests.

In any case be it business or enterprise Customers and/or in future reseller customers; when traffic analysis indicates the presence of abnormal calling patterns , our NOC is alerted which follows the defined procedures on investigating such customers.

The procedures established, and without limitation include:

1. checking recent and past call detail records and benchmark against expected trends
2. checking recent and past account activity
3. contacting the customer to understand his particular use of service and validate that the activity belongs to that customer.
 - a. In the event investigation results yield any negative connation the offending traffic, customer and/or both shall be terminated immediately by the Company.

The Company will immediately investigate suspicious activity found by its monitoring systems or reported to the Company by customers or third parties, including the ITG, all federal, state, and local regulatory commissions, and all civil and criminal law enforcement.

The investigation could potentially result in opening a traceback request with the Company contacting a customer to correct improper use of the network, or, if the customer does not respond or comply, to immediately block their use of the Company network.

In any case the Company shall respond to and shall use all best and reasonable business efforts to respond to any ITG inquiry or ticket (or any other legitimate governing state or regulatory body) within and less than twenty-four (24) hours.

In the case and when non-compliant calls come to our attention, through our own analysis or via our call mitigation and analytics vendor, we shall promptly investigate and take necessary action with the offending customer in order to mitigate ongoing illegal activity. In such case and if the call cannot be validated, we will fully reject the call being sent to our network.

The Company has an established point-of-contact for traceback and takedown requests from bona fide sources, and is committed to responding swiftly in order to maintain STIR/SHAKEN and RMD integrity. For credible requests that include sufficient supporting detail, the Company does not require a subpoena or similar documentation.

The Company Contact for any above including takedown requests is:

Name: Brandon Watts



10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095
Direct Dial Phone: 1-801-702-4249
Email: regcompliance@calltower.com

The Company will always willingly share and comply with providing as much information with industry forensics efforts and enforcement officials as is practical and legal. In recognizing that users of our network may be breaking the law need not be afforded the same privacy protections as those complying with the rules. In such case and when and as requested by law the Company will also provide all related CPNI information to any governmental authority.

The Company always employs real-time controls on traffic. All calls must have valid caller-ID values and ANI. Each customer has a calls-per-second limit commensurate with the traffic description provided and stated in the Customer Agreement and Service Order; as applicable.

The Company monitors all traffic moving through its network and looks for abnormal calling patterns. The Company is committed to being vigilant and diligent at inspection of call durations across our network to ensure that no auto-dialer traffic is being sent by any customer that signed up for the Company VoIP services. We also track call volumes and caller-ID utilization to spot changes indicative of illegal robocalls. Verify most-frequent Caller-IDs to identify any that are being misused.

At all times we also require our team and call mitigation and analytics vendor, and internal technicians to check the Certificate Revocation List (CRL) as part of their routine compliance activities.

The above stated Company Contact is also identified by our Company to be the single point of contact in charge of responding to traceback requests and respond to traceback requests as soon as possible. The same Company Contact also serves to communicate and cooperate with state Attorney General's office and other regulators about recognized scams and trends in illegal robocalling.

For all types of customers, The Company implements network-level call blocking at no cost to the Customer. The Company uses all best and reasonable efforts to ensure that all tools offered safeguard customers' personal, proprietary, and location information.

VII. COMPANY DECLARATION

The Company has not, nor has it ever been subject to any FCC Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

If any questions regarding the Company Robocall Mitigation Plan Please Contact:

CallTower, Inc.

10701 S River Front Pkwy, Suite 450, South Jordan, UT 84095

Name: Brandon Watts

Email: regcompliance@calltower.com

Direct Dial: 801-702-4249