

Brytecall LLC
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 Brytecall LLC (“Brytecall”), to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks. 47 CFR § 64.6301.

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.

Brytecall 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 Brytecall’s Robocall Mitigation plan.

II. Brytecall’s Know Your Customer (“KYC”) Standards

Brytecall is a white-labelled voice service provider that focuses its business and operations on the small and medium-sized business segment of the voice services communications market in its local service territory. As part of its customer-onboarding process, Brytecall either meets personally with or conducts an extended telephone call to discuss the prospective customer’s needs and Brytecall’s services. It undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement. Brytecall investigates the prospective customer’s background, such as checking for a company website, the amount of time the business has been open, and other indications of a legal, operating business. Brytecall routinely deploys its equipment and services at the customer’s location and therefore is privy to their usage practices. As of this filing, none of Brytecall’s business customers are call centers or other high-call-volume operations likely to generate illegal robocalls, and the end user cannot provision a device without Brytecall’s support services. Brytecall’s customers only make one-to-one calls and do not use any software or equipment to make automated calls.

Among other data points collected and, as appropriate, verified, as part of those processes Brytecall gathers the following customer-identifying facts and circumstances:

- Customer business name,
- physical business location,
- contact person(s), and
- Email address and website.

III. Brytecall's Acceptable Use Policy

As part of its customer-onboarding process, Brytecall's customers acknowledge that their use of the Services is subject to compliance with Brytecall's Acceptable Use Policy (AUP). Among other things, Brytecall's AUP prohibits:

- 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.
- 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.
- Using Brytecall's Services in any way that fails to conform to 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.
- Creating a false identity, forged email address or header, 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.

Brytecall is authorized to suspend and/or terminate all Services in the event of an AUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Brytecall has a complete STIR/SHAKEN implementation in the IP portions of its network.

Brytecall's end users only use telephone numbers to which they have subscribed from Brytecall, such that Brytecall has a documented, verified relationship between the originating end user and their telephone number(s) used to originate their calls. Further Brytecall does not allow its customers to change their Caller ID displayed on their calls, such that their Caller ID accurately reflects their assigned telephone number(s).

V. Proactive Network Monitoring

Brytecall has various monitoring and reporting systems in place in its network and via its upstream carrier to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example, Brytecall's monitoring systems are capable of assessing traffic based on various criteria, including data relating to call frequency per line (CPS), short-duration calls (ACD), answer-seizure ratios (ASR), and other anomalous call patterns.

If those systems and/or Brytecall detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Brytecall will take prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, Brytecall will block any further traffic from being carried associated with the devices of that suspicious traffic. In the event Brytecall discovers any suspicious traffic that is not demonstrably unlawful, Brytecall will complete its investigation, and their service can be temporally suspended while that process is completed depending on the severity of the complaint.

VI. Commitment to Traceback Cooperation

Brytecall 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. Brytecall will dedicate sufficient resources to provide prompt and complete responses to such requests. Brytecall will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.