

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Business Telecommunications Services, Inc. (“BTS”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. BTS reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

Company Background

BTS is a Miami-based international wholesale telecommunications service provider for U.S.-based and foreign carriers worldwide. BTS is considered both a gateway provider with a STIR/SHAKEN obligation and a non-gateway intermediate provider with a STIR/SHAKEN obligation. Its specific role at a given time is based on the factual circumstances. BTS does not originate end-user traffic. BTS maintains interconnection points in Miami, Northern Africa, Europe, and Asia. It carries traffic for over 200 carriers, including major cable multiple-system operators (MSOs) and foreign carriers who exchange traffic in their countries. Almost all traffic is exchanged in Internet Protocol (IP). BTS has been in the telecommunications business since 1993 and has held a Section 214 license from the Federal Communications Commission (FCC) since 2001.

As discussed below, BTS is implementing STIR/SHAKEN as both a gateway provider and a non-gateway intermediate provider and will sign calls consistent with STIR/SHAKEN standards and FCC rules. Because of its relationships with established carriers worldwide, BTS is not a significant source of U.S.-bound robocalls. BTS has deployed protections designed to ensure that it remains free of illegal robocalls on its network.

BTS has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, and none of its prior certifications have been removed from the Database by the Commission.

STIR/SHAKEN Implementation

BTS will comply fully with all conditions set forth in the FCC’s orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework for gateway providers and non-gateway intermediate providers.

BTS has implemented technical procedures to pass unaltered any identity header it receives with calls using Session Initiation Protocol (SIP) on the IP portions of its network to terminating voice service providers or subsequent intermediate providers in the call path. Additionally, BTS holds a service provider code (SPC) token and a certificate from a Secure Telephone Identity Certification Authority (STI-CA) and will authenticate and verify any unsigned calls it receives in a manner consistent with the standards developed under the STIR/SHAKEN framework and FCC rules. BTS also actively participates as a partner in the Industry Traceback Group (ITG) and, as discussed in greater detail below, BTS will respond to all traceback requests it receives from the FCC, law enforcement, or the ITG regarding calls for which it acts as a gateway provider or a non-gateway intermediate provider.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that BTS has implemented to detect and prevent illegal robocalls on its network. As both a gateway provider and a non-gateway intermediate provider, BTS is at risk of exchanging illegal robocalls only if it is passed such traffic from its upstream carrier customers. The measures described below explain how BTS mitigates and addresses that risk. BTS will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described below.

Upstream Carrier Customer Due Diligence

- BTS conducts a comprehensive due diligence and credit review before establishing a contractual relationship with upstream carrier customers. The due diligence procedures are described more fully in the Confidential Attachment to this Plan.
- BTS researches its upstream carrier customers' reputations and assesses the accuracy of all reported information. The procedures used are described more fully in the Confidential Attachment to this Plan.
- BTS collects sufficient information to verify upstream carrier customer information is current when contracts are renewed or services are added.
- BTS will terminate or suspend service to upstream carrier customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Contractual Provisions** – BTS contracts typically establish a reciprocal general obligation between BTS and its upstream carrier customers to not use the services for any unlawful purpose, to prevent fraudulent uses, and to cooperate with each other to avoid these unlawful activities. BTS contracts also include a fraud clause, which follows the i3forum model and stipulates the legal actions BTS can take in case of receiving fraudulent traffic. The clause establishes: (1) the definition of what constitutes fraud; (2) liability and payment rules when fraud is found; (3) a right to suspend service; (4) the ability to initiate a dispute and dispute resolution procedures; and (5) credit note handling principles.
- **Anti-Fraud Team** – BTS maintains an internal Anti-Fraud Team that coordinates anti-fraud tasks with the Customer Service and Traffic Management Departments. The Anti-Fraud Team functions 24 hours a day, 7 days a week and manages the search and detection of fraudulent traffic as well as escalation and notifications when such traffic is identified. Additional information regarding BTS's Anti-Fraud activities, including in-house monitoring and analytics, is provided in the Confidential Attachment to this Plan. BTS does not use a third-party analytics vendor.

- BTS blocks traffic from invalid numbers by default. BTS also will block traffic that appears to be illegal or is flagged as suspicious under its fraud policy. Finally, pursuant to FCC rules, BTS blocks calls from certain providers whose filings do not appear in the Robocall Mitigation Database.

Responding to Traceback Requests

- BTS has participated in the Industry Traceback Group (ITG) since 2019.
- BTS follows the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
 - **Dedicated Point of Contact** – BTS has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual, and has provided the ITG with the contact information and business hours for those individuals.
 - **Ongoing Coordination** – BTS will coordinate with the ITG and other providers in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the FCC, law enforcement, or the ITG, BTS will fully respond to the traceback request within 24 hours of receipt of the request. In the event BTS is unable to respond to a traceback request, it will provide sufficient information in the traceback portal as to why it is unable to respond.
 - **Privacy of Traceback Investigations** – BTS will not share information about traceback investigations, except with the ITG, with other providers involved in the traceback investigation, or when pursuant to a valid legal process.
- BTS maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.
- BTS will periodically review records of traceback requests to identify customers that are the subject of a pattern of traceback inquiries. BTS will determine an appropriate action to take on a case-specific basis, which may include directing the customer to remedy the problem and, if effective action is not taken, temporary suspension of the customer and/or termination of the customer's service.
- BTS maintains records of any traceback request it receives and the upstream carrier customer involved in the request.

Cooperation with State and Federal Regulators

BTS will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, BTS will:

- Respond to requests for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

Confidential Attachment to
BTS Robocall Mitigation Plan

[Redacted]