

## **STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)**

Pursuant to 47 C.F.R. § 64.6305, S and BTS Global KK (“SBTS”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. SBTS 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**

SBTS is a foreign service provider based in Japan that provides a variety of telecommunications services worldwide. As such, its official role in the call chain is as a foreign provider. SBTS on occasion uses North American Numbering Plan (NANP) numbers that pertain to the United States to send voice traffic to residential and business subscribers in the United States. Because of its relationships with established carriers worldwide, SBTS is not a significant source of U.S.-bound robocalls. SBTS has deployed the protections described in this plan to ensure that it remains free of illegal robocalls on its network.

SBTS has not been prohibited from filing in the Robocall Mitigation Database, and none of its certifications have been removed from the Database by the FCC.

SBTS has not been, at any time in the prior two years, the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to it transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

### **STIR/SHAKEN Implementation**

As a foreign service provider, SBTS is not subject to 47 C.F.R. § 64.6301, *et seq.*, or 47 C.F.R. § 64.6302, *et seq.*, including the requirements in § 64.6301(a) and § 64.6302 to implement the STIR/SHAKEN call authentication framework and authenticate caller identification information. Said differently, because SBTS is a foreign provider, the FCC does not have direct jurisdiction over the entity and cannot directly impose its STIR/SHAKEN implementation obligations upon it. The FCC recognized this lack of direct jurisdiction over foreign entities in paragraph 7 of its May 2022 Gateway Provider Order (FCC 22-37). While SBTS has not implemented STIR/SHAKEN for its calls, it has implemented a robocall mitigation plan for its calls that use NANP numbers related to the United States, as described below.

### **Robocall Mitigation Plan**

This Robocall Mitigation Plan describes the specific measures that SBTS has implemented to detect and prevent illegal robocalls on its network. The measures described below explain how SBTS mitigates and addresses the risk that it will transmit illegal robocall traffic in some capacity. SBTS 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.

### ***Customer Due Diligence***

- SBTS conducts a comprehensive due diligence review on new and renewing customers (including upstream carrier customers), confirming the customer's identity and, if it is a business, its incorporation documents. SBTS confirms the customer's service address for all customers.
- SBTS also assesses the customer's business reputation (including the reputation of telecommunications carriers from whom it receives traffic destined for the United States) and verifies this information when customer contracts are renewed or services are added.
- SBTS will terminate or suspend service to any customer with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service and not using the services for any unlawful purpose.

### ***Measures to Prevent or Avoid Exchanging Illegal Robocalls***

- **Network Monitoring.** SBTS monitors its network for fraudulent or suspicious traffic, including traffic that may be associated with illegal robocalling activity. SBTS also uses in-house analytics technology, which looks for patterns indicative of unlawful call activity, as part of this process. SBTS does not use a third-party analytics vendor.
- In the event potential fraud is detected, SBTS will take action to mitigate the potential fraud, including temporary or permanent blocking of traffic and efforts to identify the source of the traffic.
- SBTS blocks traffic from invalid NANP numbers by default. SBTS also will block traffic that appears to be illegal or is flagged as suspicious under its fraud policy. SBTS will take appropriate action with its customers upon identification of suspicious patterns of calls, including unusual volumes, and has the authority to suspend or terminate service if necessary.

### ***Responding to Traceback Requests***

- SBTS follows relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
  - **Dedicated Point of Contact** – SBTS has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual, and can provide the ITG with the contact information and business hours for those individuals.
  - **Prompt Investigation and Response** – Upon receiving a traceback request from the FCC, law enforcement, or the ITG, SBTS will aim to respond to the traceback request within 24 hours of receipt of the request, to the extent permitted under applicable law.

- **Privacy of Traceback Investigations** – SBTS will not share information about traceback investigations, except with the ITG, the FCC, and law enforcement, and to the extent permitted under applicable law.
- SBTS maintains current and correct information about its customers so that it can provide accurate responses to traceback requests.
- SBTS maintains records of any traceback request it receives and the customer involved in the request.

### ***Cooperation with State and Federal Regulators***

SBTS will cooperate, to the extent permitted under applicable law, with valid requests from the FCC or law enforcement to identify and stop any illegal robocalls that are linked to SBTS's services. Specifically, consistent with applicable law, SBTS will:

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