

SHOUTBOMB, LLC

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 C.F.R. § 64.6305, Shoutbomb, LLC, hereafter “Shoutbomb” or “Company”, submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. Company reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described herein at any time as it deems appropriate to reflect its business, its capabilities, its needs, and Federal Communications Commission (“FCC”) obligations.

Company Background

Shoutbomb is a small company that offers software which allows public and school libraries to send calls and SMS messages to their patrons. The calls and messages Shoutbomb enables are informational and they cover notifications libraries would like to send to patrons and which patrons would like to receive, e.g., updates on the books patrons have checked out or have put on hold. Moreover, the libraries are the sole decisionmakers with respect to which calls and messages to send. Currently, Shoutbomb has 61 library (i.e., end user) customers and all of these libraries are public institutions.

Shoutbomb uses Bandwidth and its network to send calls and messages on behalf of the libraries. Shoutbomb therefore lacks ultimate control over any facilities/network infrastructure necessary to implement the STIR/SHAKEN framework, and it relies on Bandwidth to satisfy any STIR/SHAKEN mandates.

Based on the foregoing, Shoutbomb does not pose a significant risk of originating illegal or unwanted robocalls. Its services are also not well suited to the origination of a high volume of calls. Shoutbomb has tailored its Robocall Mitigation Plan in light of the low risk of illegal robocalls being sent through its service. The reasonable measures Shoutbomb takes given the level of risk it faces are described in this Robocall Mitigation Plan.

STIR/SHAKEN Implementation

Shoutbomb itself has not implemented the STIR/SHAKEN call authentication framework and is unable to do so. As noted above, Shoutbomb is a small company offering software that relies on Bandwidth and its network to send calls and messages, and it therefore lacks control over the facilities and network infrastructure necessary to implement STIR/SHAKEN. Because Shoutbomb lacks this control, it is excluded from the FCC’s STIR/SHAKEN implementation obligation pursuant to paragraph 40 of the FCC’s First Call Authentication Report and Order.¹ Instead, Shoutbomb relies on Bandwidth, which owns

¹ See *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42, 35 FCC Rcd 3241, 3260, para. 40 (2020).

and maintains the network infrastructure, to implement and utilize STIR/SHAKEN authentication.

Based on the foregoing, Shoutbomb's role in the call chain is as a voice service provider without a STIR/SHAKEN obligation.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Shoutbomb has implemented to detect and prevent illegal robocalls. As a small company that offers software which allows public institutions (libraries) to send calls and SMS messages to their patrons, Shoutbomb is not a significant source of illegal robocalls. However, the measures described below explain how Shoutbomb mitigates and addresses any risks it experiences. Shoutbomb will periodically evaluate the risks it faces, the effectiveness of its current policies and procedures, and its capabilities to support the measures described. Should it determine that any changes are appropriate, its practices may differ slightly from those described below.

Customer Due Diligence

- Shoutbomb knows its customers (i.e., the libraries) by interacting directly with each of its 61 customers. Through its interactions and contracts, Shoutbomb obtains institution-specific information from each library sufficient to confirm the library's identity. This information can be used to identify a specific library should any unlawful robocalling activity occur. These practices are reasonable based on the small size of the Company.
- Shoutbomb is also given direct access to its customers' internal systems in order to help facilitate the calls and messages its customers want to send. This direct access further allows Shoutbomb to know its customers and their operations.
- Shoutbomb enters into contracts with its customers which cover the services Shoutbomb is offering. While these contracts do not contain any explicit provisions designed to mitigate illegal robocalls, they are signed by the director, assistant director, or IT manager for the specific library, providing further information on who is a responsible party serving the customer/library.

Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Know-Your-Upstream Provider** – As a software provider that helps facilitate the origination of end user calls and SMS messages, Shoutbomb does not deal with any upstream providers. All calls or messages are routed through Bandwidth's network upon origination.
- **Robocall Analytics and Blocking** – Shoutbomb relies on its partner Bandwidth to adopt any analytics software for monitoring call traffic and to block relevant calls. Shoutbomb does not use any third-party vendor(s) for analytics.
- **Monitoring** – While Shoutbomb relies on Bandwidth for its more robust analytics and monitoring capabilities, Shoutbomb also manually monitors certain traffic for patterns

indicative of illegal robocalling or messaging. Shoutbomb will sometimes review daily call/message logs provided by Bandwidth at a high level to determine if there is any problematic traffic, e.g., a large burst of calls or messages from a customer in an overly short timeframe. Upon noting any issues, Shoutbomb will contact Bandwidth to allow it to take any necessary measures.

Responding to Traceback Requests

- Shoutbomb adheres to the following best practices to facilitate its responses to any traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), including:
 - **Ongoing Coordination** – Shoutbomb will coordinate with the FCC, law enforcement, ITG, and other voice service providers in relation to instances of suspicious traffic, including exchanging information related to such traffic and follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the FCC, law enforcement, or the ITG, Shoutbomb will endeavor to fully respond to the traceback request within 24 hours of receipt of the request. In the event Shoutbomb is unable to respond to a traceback request, it will provide sufficient information as to why it is unable to respond. Shoutbomb will continue to cooperate with these entities in further investigating and stopping any illegal robocallers attempting to use its service to originate illegal calls or messages.
 - **Privacy of Traceback Investigations** – Shoutbomb 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.

Cooperation with Law Enforcement and State/Federal Regulators

Shoutbomb certifies that it has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action.

Furthermore, Shoutbomb is not currently subject to a formal Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing, nor has it been so in the past two years.

Finally, Shoutbomb commits to cooperating with state and federal regulators to help prevent any illegal robocalls or messages. Specifically, Shoutbomb will:

- Respond to requests for information about illegal robocalls or messages;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls/messages and suspicious activities; and
- Implement any new robocall mitigation procedures that are mandated, or to which Shoutbomb has committed, to the fullest extent possible.