

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

The FCC requires that all voice service providers certify in the Commission’s [Robocall Mitigation Database](#) whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, which Carrier Connection is because it has less than 100,000 lines in service, that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks.¹ 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.

Carrier Connection 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 Carrier Connection’s Robocall Mitigation plan.

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

Carrier Connection is a voice service provider that focuses its business and operations on the business segment of the voice services communications market. As part of its customer-onboarding process, Carrier Connection undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement. Carrier Connection personnel are personally involved in the customer-onboarding process, and in that connection discuss the intended use cases and needs of the prospective customers, such that it is in a position from the inception of the relationship to assess whether the prospective customer discloses any details that would suggest that their intended use case may not be lawful. Among other data points collected and, as appropriate, verified, as part of those processes Carrier Connection gathers the following customer-identifying facts and circumstances:

- Customer business name,
- physical business location,
- contact person(s), and

¹ See <https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf>; 47 C.F.R. § 64.6304.

- Email address.

III. Carrier Connection's Acceptable Use Policy

Carrier Connection's customers are required to comply with Carrier Connection's Acceptable Use Policy (AUP). Among other things, this 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 Carrier Connection'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.

Carrier Connection is authorized to suspend and/or terminate all Services in the event of an AUP violation, and commits to doing so.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Carrier Connection is diligently pursuing the deployment of STIR/SHAKEN in the IP portions of its network but has not completed that process as of the filing of this Plan. Given Carrier Connection's status as a small provider, it is subject to the Commission's two-year extension. In cases where Carrier Connection's end users use telephone numbers to which they have subscribed from Carrier Connection, Carrier Connection has a documented, verified relationship between the originating end user and their telephone number(s) used to originate their calls. In the cases where a Carrier Connection end user is using numbers secured from a different service provider, the customer has represented to Carrier Connection a right to use the telephone number at issue.

V. Proactive Network Monitoring

Carrier Connection 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 or other potentially unlawful usage. For example, Carrier Connection's network and monitoring systems are capable of assessing traffic based on various criteria, including data relating to short-duration calls, answer-seizure ratios, and other anomalous call patterns.

If Carrier Connection detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Carrier Connection 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, Carrier Connection will block any further traffic from being carried from the source of that suspicious traffic. In the event Carrier Connection discovers any suspicious traffic that is not demonstrably unlawful, Carrier Connection 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

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