



CCI NETWORK SERVICES, LLC

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 CFR § 64.6305, CCI Network Services, LLC, hereafter “CCI”, submits this report, as of **November 9, 2023**, on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. CCI 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

Founded in 2004, CCI is a leader in single-source telecommunications consulting and support in the design, provisioning, and management of custom voice and data network solutions. CCI strategically matches its customers’ needs with its multi-carrier portfolio of services giving customers the best solutions for the best overall cost. CCI’s solutions include, *inter alia*, VoIP, PBX, conference calling, and long-distance solutions.

For further identification, CCI’s FCC Operating Company Number is **663J**.

STIR/SHAKEN Implementation

Due to its various lines of business, CCI plays multiple roles in the call chain.

Because CCI resells service to end users (i.e., business customers) and wholesales service to other carriers, it is considered a voice service provider with a STIR/SHAKEN obligation that both serves end-users and acts as a wholesale provider originating calls. With respect to implementation, CCI has partially implemented the STIR/SHAKEN call authentication framework because its current voice traffic is comprised of both TDM and SIP service.

CCI is also considered a non-gateway intermediate provider with a STIR/SHAKEN obligation.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that CCI has implemented to detect and prevent illegal robocalls as of **November 9, 2023**. Specifically, CCI is at risk of unintentionally exchanging illegal robocalls when originating traffic on behalf of others, and when passing traffic from immediate upstream providers in its role as a non-gateway intermediate provider. The measures described below explain how CCI mitigates and addresses these risks, recognizing that it is impossible to prevent all illegal robocalls. CCI 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 slightly from those described below.

Customer and Upstream Provider Due Diligence

- CCI uses a vetting process for all customers¹ under which the customer must complete a questionnaire and a third-party vendor performs a background check.
 - The questionnaire obtains relevant background information, including but not limited to, the customer's name, type of business, headquarters address, website address, and company contacts. It also asks about the types of voice services provided by the customer.
 - The questionnaire asks robocall and mitigation focused questions, including but not limited to, whether anyone generates auto-dialed traffic, if the customer participates in the traceback process, if the customer has filed in the Robocall Mitigation Database, and if the customer has implemented STIR/SHAKEN. Relatedly, it asks if the customer has implemented a robocall mitigation plan and for the customer to describe any steps it has taken to avoid originating illegal robocalls.
 - Under the questionnaire, the customer must certify that it has knowledge of the U.S. laws prohibiting the generation and transmission of illegal, harassing, or unwanted voice calls, and that it complies with these laws and consents to disclose certain details if there are potential violations of these laws. The customer must also certify that it will respond promptly to traceback requests and take steps to address illegal traffic transmitted using its network.
- CCI has relevant customers attest that they have the right to use certain telephone numbers and they will strive to not terminate illegal robocalls.
- In some instances, CCI's larger customers are met with personally by CCI staff to determine the nature, needs, and reputation of the relevant customer's business.
- CCI also monitors the use of its services for potential violations of contractual obligations or provisions relating to acceptable use of service. Under agreements it enters with customers, CCI is empowered to take any action consistent with state and federal law that it deems appropriate to prevent fraud or abuse in connection with its services.

¹ "Customers" in this due diligence section include immediate upstream providers on whose behalf CCI passes traffic as a non-gateway intermediate provider.



Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Monitoring and Blocking** – CCI uses pattern recognition software and continuously monitors traffic from existing customers for patterns of known abuse and illegal robocalling. Some of the patterns CCI monitors for include:
 - Large bursts of calls in a short timeframe;
 - Low average call duration;
 - Low call completion ratios; and
 - Dialed numbers appearing on the National Do Not Call Registry.
- Upon noting these patterns, CCI will review the traffic and take immediate action where necessary to prevent illegal robocalling or other forms of fraud or abuse. Actions include blocking of traffic and suspension or termination of service. Pursuant to FCC rules, CCI will also block calls from providers whose filings do not appear in the Robocall Mitigation Database.
- **Analytics and Security** – CCI does not utilize any third-party analytics vendors at this time. However, it does engage in monitoring and pattern recognition as described above, and it has implemented session border controllers and specific security mechanisms for additional protection. These include:
 - Imposing concurrent call limitations to address large bursts of calls in a short timeframe;
 - Monitoring the number of ports; and
 - Imposing limits on trunk groups.

Responding to Traceback Requests

- CCI adheres to the following best practices to facilitate its responses to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), including:
 - **Dedicated Point of Contact** – CCI has designated an individual as a point of contact for addressing traceback requests.
 - **Ongoing Coordination** – CCI 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 ad hoc follow-up as appropriate.

- **Prompt Investigation and Response** – Upon receiving a traceback request from the FCC, law enforcement, or the ITG, CCI will fully respond to the traceback request within 24 hours of receipt of the request. In the event CCI is unable to respond to a traceback request, it will provide sufficient information as to why it is unable to respond. CCI will continue to cooperate with these entities in further investigating and stopping any illegal robocallers attempting to use its services to originate, carry, or process illegal calls.
- **Privacy of Traceback Investigations** – CCI 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.
- CCI will periodically review records of traceback requests to identify customers that are the subject of repeated traceback inquiries. CCI will determine an appropriate action to take on a case-specific basis, which may include working with the customer to mitigate illegal traffic, blocking the customer's illegal traffic, temporary suspension of the customer, or termination of the customer's service.
- CCI maintains records of any traceback requests it receives, including the relevant parties involved in the requests.

Cooperation with Law Enforcement and State/Federal Regulators

CCI certifies that it has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action. CCI will provide information on its principals, affiliates, subsidiaries, and parent companies to allow the FCC to confirm that CCI has not been prohibited from filing in the Robocall Mitigation Database once the FCC has decided on the form and format of this data. Currently, CCI does not have any affiliates or subsidiaries, and it is majority owned by a private equity firm.

Furthermore, CCI is not currently subject to a formal Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing or a deficient Robocall Mitigation Database certification or mitigation plan, nor has it been so in the past two years. The same is true for any entities affiliated with CCI.

Finally, CCI commits to cooperating with state and federal regulators to help prevent illegal robocalls. Specifically, CCI 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 any new robocall mitigation procedures that are mandated, or to which CCI has committed, to the fullest extent possible.