CONTACT CENTER SPECIALISTS 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 Contact Center Specialists LLC ("CCS"), 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, by June 30, 2021, in the Commission's Robocall Mitigation Database whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, as CCS is under 47 C.F.R. § 64.6304 as a small provider, 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.[2] CCS 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 CCS's Robocall Mitigation plan, and supersedes its initial filing in the FCC's database.

II. CCS's Know Your Customer ("KYC") Standards

CCS is a UCaaS software and voice services provider that focuses on the business end user customer segment of the communications market, particularly those in the contact-center industry. As part of its customer-onboarding process, CCS undertakes various commercially reasonable precautions to verify a given customer's identity as part of entering into a formal written agreement, and soliciting information from the prospective customers designed to solicit the customer's acknowledgement and recognition that their use of the services is subject to a robust legal and regulatory regime affecting their outbound calling practices.

All prospective customers undergo an onboarding process that is personally conducted by CCS personnel that includes phone calls with the prospective customer. New customers cannot enter into an agreement for CCS's services without going through that personalized onboarding process; i.e., there are no online-only subscribers to CCS's services.

---

[1] *See* https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf.

[2] FCC Public Notice, Wireline Competition Bureau Issues Caller ID Authentication Best Practices, WC Docket Nos. 17-97 and 20-324, DA 20-1526, at ¶ 20 (Dec. 22, 2020).

As part of that personally reviewed process, CCS personnel investigate the prospective customer's background, such as checking for valid contact information tied to the company subscribing to the services. Among other data points collected and, as appropriate, verified, the following customer-identifying facts and circumstances are gathered:

- Customer business name,
- Company email and phone number,
- Company business address and state of incorporation, and
- Company personnel contact name.

CCS's onboarding process also includes the prospective customer's completion of a detailed new-customer questionnaire that solicits details on the customer's anticipated use cases of the CCS services, along with a confirmation that they acknowledge the various legal restrictions and conditions surrounding their use of the CCS platform.

While CCS does not provide any wholesale voice services to other telecommunications providers, in the event CCS provides any wholesale services to other voice service providers, its verification practices will also include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers and the Commission's Robocall Mitigation Database.

III. CCS's Acceptable Use Policy

As part of its customer-onboarding process, CCS's customers contractually agree to various terms and conditions, and their usage of CCS's services is subject to CCS's Acceptable Use Policy (AUP). Among other things, CCS's contract and AUP prohibit:

- 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 CCS'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.

CCS's contracts with its customers stipulate that CCS is authorized to suspend and/or terminate all Services in the event of a violation of these terms or any other unlawful conduct committed through their use of the services.

IV. STIR-SHAKEN Capabilities and Telephone Number Authorization

CCS 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. It has now secured its OCN from NECA, and is proceeding with the STI-PA and Certificate Authority contracting and network-implementation processes, which it anticipates completing in the first quarter of 2022, barring unforeseen circumstances. Given CCS's status as a small provider, it is subject to the Commission's two-year extension under 47 C.F.R. § 64.6304. In the interim, most of CCS's downstream carriers are attesting CCS's end users' calls in accordance with their STIR/SHAKEN policies and deployments.

CCS's end users are only authorized to use and display as their Caller ID the telephone numbers to which they have subscribed from CCS, such that CCS has a documented, verified relationship between the originating end user and their telephone number(s) used to originate those calls. If CCS discovers that an end user has manipulated their Caller ID parameters to display a number not assigned to them by CCS, CCS's policy is to give the customer one warning about that infraction and then terminate the end user's services in the event of a second such infraction.

V. Proactive Network Monitoring

In addition to the significant manual review of customers' background and use cases described above, CCS 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, CCS at a network level applies calls-per-second and session limits on all end user accounts, and because the end users are using CCS's UCaaS software as part of its call campaigns, it can access certain additional information, such as recordings and other details, available in the platform. routinely analyzes message delivery rate data as the best indicia of potentially suspicious or unwanted traffic, and promptly investigates that customers' traffic. Any Traceback requests, subpoenas, carrier complaints or similar events likewise trigger a prompt investigation by the company into that customers' traffic, and it is CCS's practice and policy to respond to all tracebacks and similar enforcement authority requests within 24 hours.

VI. Commitment to Traceback Cooperation

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

CCS Robocall Mitigation Plan v. 2, effective October 15, 2021