

Certain Communications Corporation
FRN 0018463968

Robocall Mitigation Program

February 2024

Table of Contents

I.	Robocall Mitigation Program Introduction	1
A.	Company Summary	1
B.	Filing of RMP and Implementation of STIR/SHAKEN	1
C.	Regulatory Actions, Investigations and RMD Filing Status	1
II.	Robocall Mitigation Program	2
1.	Implementing Knowing Your Customer Protocols	2
2.	Requiring Contractual Provisions to Mitigate Illegal Robocalls	2
3.	Only Accepting Traffic from Providers in the RMD	3
4.	Blocking Calls on a Do-Not-Originate List	3
5.	Analyzing and Monitoring Network Traffic Routing Through CCC's Network.....	3
6.	Ensuring Foreign Providers Are Not Using CCC to Carry or Process High-Volume Illegal Traffic onto the U.S. Network	4
7.	Authenticating Voice Traffic	4
8.	Responding to Commission, Law Enforcement and ITG Traceback Requests	4
9.	Designating an Employee Responsible for Addressing Robocall Mitigation- Related Issues	5
10.	Updating CCC's RMD Submission and RMP	5

I. Robocall Mitigation Program Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Program (“RMP”) details the policies and practices that Certain Communications Corporation (“CCC”), FRN 0018463968 has established to prevent unlawful robocalls from originating on, terminating to, or routing through its voice network where it is operating as a Voice Service Provider, a Non-Gateway Intermediate Provider, and/or a Gateway Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R § 64.6300.

A. Company Summary

CCC is a provider of wholesale VOIP communications services for terminating voice traffic in the United States and the extended North American footprint. With its commercial offerings, CCC enables service providers and businesses to transact and communicate with their customers by accessing the networks of voice service providers that are capable of reaching the phones of individuals and businesses. Depending on the services provided, CCC may serve as a Voice Service Provider, a Non-Gateway Intermediate Provider, and/or a Gateway Provider.

CCC is an S- Corporation registered in the state of Delaware. CCC owns and operates technical infrastructure in order to align with technical and regulatory compliance requirements and infrastructure for the authentication of voice traffic with STIR/SHAKEN.

B. Filing of RMP and Implementation of STIR/SHAKEN

CCC has fully implemented STIR/SHAKEN and has submitted its certification that all voice traffic that transits its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. § 64.6301(a). In accordance with the RMD 12/2022 Filing Instructions, FCC Rule 47 C.F.R. § 64.6305(b) and because CCC is a “Combined Gateway and Voice Service Provider” under these instructions, CCC has certified that CCC has “fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with FCC Rule, 47 C.F.R. § 64.6302(b).” In addition, CCC has uploaded this RMP into the RMD because it “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic” and has included “a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.”

C. Regulatory Actions, Investigations and RMD Filing Status

CCC is not subject to any Federal Communications Commission, law enforcement, or regulatory agency actions or investigations and has not had its authority to file in the RMD revoked.

II. Robocall Mitigation Program

This RMP applies to CCC calling platforms and provides information on CCC policies and procedures on the following topics that are discussed in turn below which “details the specific reasonable steps CCC has taken to avoid carrying or processing illegal robocall traffic”:

- (1) Implementing Know Your Customer Protocols
- (2) Requiring Contractual Provisions to Mitigate Illegal Robocalls
- (3) Only Accepting Traffic from Providers in the RMD
- (4) Blocking Calls That Are Identified by Downstream Carriers That Are On Do-Not-Originate Lists
- (5) Analyzing and Monitoring Network Traffic Routing Through CCC’s Network
- (6) Ensuring Foreign Providers Are Not Using CCC to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (7) Authenticating Voice Traffic Originated by CCC Customers
- (8) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (9) Designating an Employee Responsible for Addressing Robocall Mitigation-

Related Issues

- (10) Updating CCC’s RMD Submission and RMP

1. Implementing Knowing Your Customer Protocols

Consistent with the FCC’s Caller ID Authentication Best Practices No. 1 and 47 C.F.R. § 64.1200(n)(3), CCC vets “the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.” In so doing, CCC takes “affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.” In this regard, CCC has implemented appropriate Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. As part of its KYC protocols, CCC requires any customer to provide sufficient information to ensure its legitimacy. Among other things, CCC generally requires its customers to provide the full legal name of the company, state or country of incorporation, the physical address of its operations, the billing name and address (when different), and the customer contact name and telephone number, and nature of the customer’s business. As indicated in Section 3, below, if the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, CCC confirms, in accordance with currently effective FCC rules, that the company is appropriately listed in the FCC’s RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.

2. Requiring Contractual Provisions to Mitigate Illegal Robocalls

Voice service customers of CCC are subject to robust terms and conditions that (1) obligate customers not to use CCC’s services for unlawful purposes; and (2) preserve CCC’s right to terminate customers for violations of the law.

CCC's contracts include terms that forbid the customer from using CCC's services to originate and/or otherwise transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act ("TCPA") and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ("TRACED Act") and/or the rules promulgated pursuant to these statutes. CCC's contract terms provide that if any calls originated or otherwise transmitted by the customer to CCC violate the TCPA, the TRACED Act, or the rules promulgated under these statutes, then CCC may, at its sole discretion, suspend or terminate the customer's service immediately, among other remedies.

3. Only Accepting Traffic from Providers in the RMD

Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(e)(1), CCC accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers and Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(e)(2), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), CCC accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(e)(3), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), CCC accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD showing that the Gateway Provider has affirmatively submitted its filing and RMP, and (b) has not been de-listed pursuant to an enforcement action.

4. Blocking Calls On a Do-Not-Originate List

CCC blocks calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan numbers. CCC has protocols in place to detect DNO calls and once identified, block calls that are attempted where the originating number is a DNO number. CCC is utilizing the DNO list offered by US Telecom.

5. Analyzing and Monitoring Network Traffic Routing Through CCC's Network

Upon receiving call traffic, CCC also analyzes and monitors the call traffic that originates on, terminates to, or routes through CCC's voice network. CCC monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling. In this regard, CCC has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, and atypical call activity), investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis. When analyzing and monitoring call traffic, if CCC discovers call patterns that are consistent with illegal robocalling, CCC, after further investigation, takes appropriate action to address such behaviors, which may include working with the originating customer to resolve problematic traffic, blocking the problematic calls and/or terminating the customer's service.

6. Ensuring Foreign Providers Are Not Using CCC to Carry or Process High-Volume Illegal Traffic onto the U.S. Network

Pursuant to 47 C.F.R. § 64.1200(n)(4) and its January 16, 2023 effective date, when CCC serves as a Gateway Provider for voice traffic that is routing through its network, CCC takes reasonable and effective steps discussed under Section 5, above, to ensure that any Foreign Voice Service Provider or Foreign Intermediate Provider from which CCC directly receives traffic is not using CCC, as a Gateway Provider, to carry or process a *high volume* of illegal traffic onto the U.S. network. CCC will block all calls which are not authenticated, prior to arrival to the CCC network, using STIR/SHAKEN.

7. Authenticating Voice Traffic

When operating as a Voice Service Provider, CCC does requires its customers to provide valid caller identification information when sending calls to CCC's platform that will be exchanged with another Voice Service Provider or Intermediate Provider and, to the extent technically feasible, transmits that call with the caller identification information to the next Voice Service Provider or Intermediate Provider in the call path.

When operating as an Intermediate Provider, CCC passes unaltered, any authenticated caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field. With respect to any unauthenticated calls it receives, CCC is excused from authenticating such calls as CCC participates cooperatively with the industry traceback consortium and responds fully and in a timely manner to all traceback requests it receives from the Commission, laws enforcement, and the industry traceback consortium.

When operating as a Gateway Provider, CCC authenticates caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call.

8. Responding to Commission, Law Enforcement and ITG Traceback Requests

CCC is committed to ensuring that its network is not utilized for the origination, termination or routing of unwanted and illegal robocalls. In accordance with the FCC's regulations 47 C.F.R. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), CCC will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium ("ITG") within-24 hours (this 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1)(ii) and as clarified by the Commission) and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use CCC's network to carry or process calls. As part of this commitment, CCC will take the necessary steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules. CCC works with ITG and typically responds within 8 hours to ITG traceback requests.

9. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure CCC's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, CCC provides the following name, title, department, business address, telephone number, and email address of the individual within CCC that leads CCC's handling of robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: Vincent Arena

Contact Title: President

Contact City: Denver

Contact State and Zip Code: Colorado, 80246

Contact Telephone Number: 310-365-2168

Contact Emails: varena@certaincorp.net, copy to: corporate@certaincorp.net

10. Updating CCC's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), CCC will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.