



Comcast IP Phone, LLC
Comcast Phone of California, LLC
Comcast Phone of Texas, LLC
Robocall Mitigation Plan

Introduction

This document details the “reasonable steps” that Comcast IP Phone, LLC, Comcast Phone of California, LLC, and Comcast Phone of Texas, LLC and certain business units of these entities and their affiliates¹ have taken to avoid the origination, carrying, and/or processing of illegal robocall traffic. Among other things, this document describes the analyses that are performed and actions taken by Comcast to identify sources of voice traffic that are likely to be associated with illegal robocalls; to pre-qualify prospective retail and wholesale customers and peering partners; to monitor existing customers and partners for traffic patterns and other information indicative of the potential for transmitting illegal robocalls; and to mitigate the acceptance and transmission of illegal robocall traffic on the Comcast network.

Comcast is committed to responding fully and within 24 hours to all traceback requests from the Commission, law enforcement agencies, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping illegal robocallers that use or transmit traffic to Comcast’s network.

A. Know Your Customer

Comcast employs a variety of know your customer (“KYC”) initiatives, tailored according to service type and the prospective customer’s role in the call path.

For retail VoIP services offered through Xfinity Voice, prospective customers are required to provide contact details and related information, which is confirmed via national credit reporting agencies. Additionally, all such customers are subject to the Xfinity Residential Services Agreement and Acceptable Use Policy (“AUP”), which together expressly prohibit customers from using the service to engage in auto-dialing, telemarketing, or any other activities that do not consist of standard residential voice calling involving live dialogue between individuals. The Agreement and AUP reserves Comcast’s right to suspend and/or terminate service for violations of these and other terms and conditions.

For retail VoIP services offered to businesses through Comcast Business, sales agents are provided with materials to assist them in evaluating the potential for a prospective customer to use the service to engage in illegal robocalling, rather than only for legal purposes. Moreover, all Comcast Business customers are required to sign a Service Order Agreement accepting Comcast’s terms and conditions and the AUP relevant to the voice services ordered, which generally prohibit using the services to engage in illegal robocalling and other forms of abusive calling.

For syndication solutions that provide other multiple system operators (“MSOs”) with a wholesale voice platform that they can offer to their own customers, Comcast contractually

¹ This Robocall Mitigation Plan for Comcast IP Phone, LLC, Comcast Phone of California, LLC, and Comcast Phone of Texas, LLC and the accompanying certifications in the FCC’s Robocall Mitigation Database for these entities also cover the following business units of these entities and their affiliates: Xfinity Voice, Comcast Business, Comcast Technology Solutions, and Comcast Voice Syndication. Comcast IP Phone, LLC, Comcast Phone of California, LLC, and Comcast Phone of Texas, LLC and the business units of these entities and their affiliates are collectively referred to as “Comcast” in this submission.

requires the downstream MSO to prohibit illegal robocalling and other abusive calling practices. Such contracts also establish the parameters of and procedures for Comcast's monitoring to identify suspicious or possibly fraudulent traffic from or illegal robocalling activity by the downstream MSO's own customers.

For wholesale traffic exchange and call termination services provided to other voice service providers, Comcast's KYC initiatives are described in the following section.²

B. Know Your Upstream Provider

Comcast undertakes extensive "know your upstream provider" efforts for prospective wholesale termination services customers and peering partners to minimize the possibility that these entities might transmit illegal traffic to Comcast's network. These efforts include:

Reputational Research. Research is conducted on prospective wholesale customers and peering partners to identify those known or that are likely to be engaged in fraudulent activities. Comcast consults regulatory and enforcement agency websites and databases as well as information that is in the public domain. In particular, Comcast researches the qualification or disqualification of prospective wholesale customers and peering partners using publicly available information from sources such as:

- The FCC's Form 499 database;
- The FCC's Robocall Mitigation Database and Intermediate Provider Registry;
- FCC and Enforcement Bureau public notices;
- FTC enforcement order and notices;
- Secretaries of state records; and
- General Internet searches for entities' involvement with fraudulent activities.

The results of such research are used as part of the vetting process for prospective wholesale customers and peering partners. In addition, screening interviews are performed to understand the business model of a prospective wholesale customer or peering partner and the risk that such an entity would engage in fraudulent robocalling schemes.

Contractual Obligations. Comcast imposes contractual obligations that prohibit the transmission of fraudulent traffic and other traffic exhibiting signs of unlawful behavior, and reserves the right to terminate service if such traffic is transmitted.

² Comcast Phone of Texas, LLC is limited to operating as an intermediate voice service provider to a single company, Eastex Telephone Cooperative. Comcast Phone of Texas, LLC does not onboard any new customers, and its monitoring of traffic in connection with its existing customer comports with the practices described below.

C. Analytics-Based Tools and Other Robocall Mitigation Techniques

Comcast relies on various analytics-based tools and other techniques to identify and mitigate illegal robocalling, including:

Network-Level Blocking. Comcast's tools automatically screen, alarm, report, and reject at the network edge calls with indicia of fraudulent robocalling or that originate from numbers on Do-Not-Originate ("DNO") lists or from invalid or unallocated numbers.

Customer-Optional Comcast-Developed Tools. Comcast offers various proprietary tools to enable its voice customers to efficiently and effectively manage their receipt of calls, including:

- Anonymous Call Rejection, which enables a customer to automatically reject calls where the caller has chosen to prevent the display of the caller's name and number;
- Selective Call Rejection (also known as Call Screening), which enables a customer to create a list of telephone numbers that will not ring through to the customer's phone; and
- Spam Blocker, which uses third-party analytics provided by Transaction Network Services Inc. to gauge the likelihood of spam and gives call recipients the flexibility to choose how they want to treat inbound calls, including through the use of Audio CAPTCHA, which requires unknown callers to enter a code to proceed.

Call Authentication Technology. Comcast has fully implemented the STIR/SHAKEN call authentication framework across its entire network, and Comcast adheres to the applicable FCC rules and industry standards for call authentication in its capacity as a retail voice services provider, non-gateway intermediate provider, and gateway provider. In addition, Comcast's Verified Caller ID displays the word "Verified" (or the character "[V]") if the caller's voice provider has authenticated the telephone number, while suspicious calls are displayed to call recipients with the prefix "Spam?" in their caller ID display.

Traffic Monitoring. Customers' traffic is monitored, and any unusual, suspicious patterns that are identified are analyzed for potential fraud, and initiates mitigation measures and conducts customer outreach if data suggests improper activity is occurring.

Principals, Affiliates, Subsidiaries, and Parent Companies

Comcast IP Phone, LLC, Comcast Phone of California, LLC, and Comcast Phone of Texas, LLC are wholly owned subsidiaries of Comcast Corporation, a publicly traded corporation whose Chairman is Brian Roberts and whose Co-Chief Executive Officers are Mr. Roberts and Michael Cavanagh.

Affiliates of Comcast IP Phone, LLC, Comcast Phone of California, LLC, and Comcast Phone of Texas, LLC that voice service providers and filers in the Robocall Mitigation Database are as follows:

Comcast OTR1, LLC
Masergy Cloud Communications, Inc.
Midcontinent Communications
Network Innovations, LLC