



Network Innovations, LLC dba Nitel
Robocall Mitigation Plan

Introduction

This document details the “reasonable steps” that Network Innovations, LLC dba Nitel (“Nitel”) has taken to avoid the origination of illegal robocall traffic as part of its robocall mitigation program.

Nitel is a wholly owned subsidiary of Comcast Corporation that offers wholesale and retail point-to-point data services and Voice over Internet Protocol (“VoIP”) services to business customers. Nitel’s VoIP services are predominately provided on a resold basis, and in such cases, the company does not own or operate the networks associated with these services, nor does it have access to the underlying networks for monitoring, detection, or authentication activities. Instead, Nitel’s underlying network providers are responsible for the monitoring for and detection of robocalling activity on their networks; blocking traffic in compliance with FCC rules and orders; responding to traceback requests within required timeframes; responding to subpoenas and other requests from law enforcement agencies; implementing STIR/SHAKEN and authenticating and verifying calls in accordance with FCC rules and orders; and undertaking “know your upstream provider” diligence. Nitel uses its own IP-based network to provide VoIP services to a small percentage of its customers, and Nitel has fully implemented STIR/SHAKEN where it has control over the network infrastructure necessary for such implementation.¹

In its capacity as a reseller, Nitel works closely with its underlying network providers to ensure that all of its customers receive the benefits of the robocall mitigation, call authentication, and other related activities performed with respect to the underlying networks. And in all events, Nitel undertakes various efforts of its own, described below, to identify and disqualify businesses as customers that are likely to be associated with illegal robocalls; to pre-qualify prospective customers that are unlikely to generate illegal robocalls; and to monitor existing customers for activities indicative of the potential for transmitting illegal robocalls.

Nitel is committed, in cooperation with its underlying network providers where relevant, 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 any illegal robocallers that use Nitel’s VoIP services to originate calls.

A. Know Your Customer

Nitel employs a variety of know your customer initiatives. Among other efforts, screening interviews are performed to understand prospective customers’ business models and the potential, or lack thereof, for involvement in illegal robocalling schemes. Nitel’s sales

¹ Because Nitel has fully implemented STIR/SHAKEN on its own network, Nitel has selected the “Complete STIR/SHAKEN Implementation” certification in the accompanying form. Where Nitel provides service over the resold facilities of other network operators, it is subject to an exemption from compliance with the STIR/SHAKEN implementation obligations in 47 C.F.R. § 64.6301(a). See *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573 ¶ 45 (2023); *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 ¶ 40 (2020); see also 47 C.F.R. § 64.6304.

department inquires about the prospective customers' background, including principals, location, and relevant qualifications. Nitel's Credit and Collections department consults with a credit reporting agency to verify information provided by the prospective customer. Nitel does not accept as customers business that provide incomplete, inaccurate, or inconsistent information. Moreover, businesses that Nitel determines are or have been associated with individuals or entities that have engaged in illegal robocalling are not accepted as customers, and existing customers identified as having such relationships may face service termination.

In addition, all Nitel customers are required to adhere to the terms and conditions of the company's VoIP services, which strictly prohibit using the services to engage in illegal robocalling.

B. Know Your Upstream Provider

Nitel has longstanding relationships with several underlying network providers on which the company relies to provide resold VoIP services to its customers, and these partners also serve as Nitel's "upstream" providers by enabling connectivity to other third-party providers. Nitel's master service agreements with these underlying network providers require them to comply with the TRACED Act and the FCC's related rules and orders. In addition, these underlying network providers have provided Nitel with written assurances that they do and will continue to sign calls originated on behalf of Nitel customers per industry standards and will abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services to Nitel. Nitel and its upstream underlying providers have further agreed to work together diligently to mitigate illegal robocalls, including cooperating when receiving and responding to traceback requests.

In the limited cases in which Nitel provides VoIP services to customers using its own network, the company undertakes extensive "know your upstream provider" efforts to minimize the possibility that these entities might transmit illegal traffic to Nitel's network. Among other efforts, if Nitel detects any indication that a specific upstream provider is transmitting illegal robocall traffic inbound to Nitel customers, Nitel may initiate a traceback investigation, contact the provider, or take direct action to mitigate against calls reaching Nitel customers.

C. Analytics-Based Tools and Other Robocall Mitigation Techniques

Nitel customers benefit from various robocall mitigation efforts undertaken by Nitel and its underlying network providers, including:

Traffic Monitoring. Nitel and its underlying network providers examine call detail records on a continuous basis to identify and address suspicious call activity and patterns. Nitel also evaluates outbound customer traffic for excessive or abnormally high outbound call volumes in short timeframes, sudden spikes in usage, short call durations, low call-completion percentages, calls made to sequential telephone numbers, and other calling behavior that is atypical for a given customer.

In addition, where Nitel detects the transmission of potentially illegal robocalls to Nitel's customers or on its network, the company undertakes an investigation to identify the providers

and/or parties involved and initiate robocall mitigation efforts. Such investigations may entail initiating traceback requests, verifying that the originating customer is authorized to use the caller ID number at issue, and determining whether the caller ID name sent to the receiving party matches the customer's corporate or d/b/a name. Where Nitel's underlying network providers or vendors identify illegal robocalling or other abusive calling practices involving Nitel's customers, the company is alerted to such activities. In all cases, Nitel takes appropriate action to address instances of illegal robocalling and other forms of abusive calling, including suspending or terminating service or blocking a non-customer's ability to terminate calls to Nitel customers, and notifying appropriate law enforcement agencies.

Telephone Number Screening. Nitel uses telephone number-based caller identity, in which the originating telephone number uniquely associated with a customer is included in call signaling used to identify the calling party, for screening purposes. Accordingly, a Nitel customer is permitted to use a telephone number as its caller identity only if the number is directly managed by Nitel, or obtained by Nitel from its underlying network providers for use by the customer. Moreover, for customers with multi-line telephone systems, Nitel and its underlying network providers have implemented an automated and secure method of validating originating telephone numbers to help ensure that a call's originating telephone number matches one of the telephone numbers assigned to the customer.

Traceback Requests. Upon receipt of a traceback request, Nitel's dedicated traceback team opens a ticket with Network Operations and Nitel Management is notified. If a traceback identifies an existing Nitel customer as a source of illegal robocalls, or as having transmitted illegal robocalls, the company requests information from the customer about the activities at issue and verification that the customer is taking steps to mitigate such traffic. If the customer does not take remedial measures, fails to respond to such a request in a timely manner, or does not provide an adequate explanation for the traffic at issue, Nitel reserves the right to block all traffic originated by the customer.

Principals, Affiliates, Subsidiaries, and Parent Companies

Network Innovations, LLC is a wholly owned subsidiary 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 Network Innovations, LLC that are voice service providers and filers in the Robocall Mitigation Database are as follows:

Comcast IP Phone, LLC
Comcast Phone of California, LLC
Comcast Phone of Texas, LLC
Comcast OTR1, LLC
Masergy Cloud Communications, Inc.
Midcontinent Communications