



Robocall Mitigation Program

Principals, Affiliates, Subsidiaries, and Parent Companies

Etex Telephone Cooperative, Inc., the filing entity, is the parent company to its two subsidiaries, which are Etex Communications, LLC and Etex Celltel, LLC. Etex Telephone Cooperative, Inc. owns 100% of both subsidiaries. Etex Telephone Cooperative, Inc., has no principals or affiliates. Charlie Cano is the CEO and has Managing Control of Etex Telephone Cooperative, Inc. and all its subsidiaries.

Company Name	Relationship to Filing Entity	Type of Company	% Owned by Filing Entity	Management or Control of the Entity
Etex Telephone Cooperative, Inc.	Parent	ILEC	0%	Charlie Cano - CEO and General Manager
Etex Celltel, LLC	Subsidiary	Holding	100%	Charlie Cano - CEO and General Manager
Etex Communications, LLC	Subsidiary	CLEC	100%	Charlie Cano - CEO and General Manager

STIR/SHAKEN Implementation

All the voice traffic that originates on Etex Telephone Cooperative Inc.'s "Etex" network is subject to the robocall mitigation program described below.

Etex Telephone Cooperative, Inc. has upgraded its network and fully implemented STIR/SHAKEN authentication framework in its Internet Protocol portions of its network. In accordance with 47 CFR § 64.6301(a), Etex is fulfilling its obligation by authenticating and verifying caller identification information for all SIP calls that exclusively transit its own network, authenticating caller identification information for all SIP calls it originates and that it will exchange with another voice provider or intermediate provider and, to the extent technically feasible, transmitting that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path and by verifying caller identification information for all SIP calls it receives from another voice service provider or intermediate provider which it will terminate and for which the caller identification information has been authenticated.

The non-IP portions of its network rely on technology that cannot initiate, maintain, carry, process or terminate SIP calls are deemed subject to a continuing extension, as noted below.

STIR/SHAKEN Extensions

Etex qualifies for the FCC's continuing extension of the STIR/SHAKEN implementation requirement for the non-IP portions of its voice network pursuant to 47 CFR § 64.6304(d). Certain segments of Etex's network utilize legacy, non-IP technology and interconnect with upstream carrier facilities that do not currently support full end-to-end SIP functionality. Because IP-based authentication requires SIP signaling across the call path, these interconnection limitations prevent full implementation of STIR/SHAKEN on those portions of the network.

Consistent with 47 CFR § 64.6303(a)(2), Etex participates in industry-led efforts addressing caller identification authentication for non-IP network segments through membership in national and state telecommunications associations and through coordination with its network equipment vendor and carrier partners. These engagements support the development and evaluation of non-IP caller ID authentication solutions applicable to Etex's network environment.

Specific Reasonable Steps Taken to Avoid Originating Illegal Robocall Traffic

Listed below are the specific reasonable steps that Etex is taking to avoid originating illegal robocall traffic.

1) Know Your Customer (KYC) Policy *(In accordance with 47 C.F.R. § 64.1200(n)(4))*

Etex has implemented a Know Your Customer (KYC) Policy designed to take affirmative and effective measures to prevent new and renewing customers from originating illegal or fraudulent robocall traffic on its network. As part of this process, Etex verifies the identity and legitimacy of customers during onboarding and renewal, including review of customer information, stated business purpose, and anticipated traffic patterns, prior to provisioning service.

Etex incorporates contractual provisions prohibiting illegal robocalls and requiring customer cooperation with investigations, traceback requests, and corrective actions when suspect traffic is identified. Etex monitors customer-originated traffic using call analytics to identify unusual, high-risk, or suspicious calling behavior and investigates suspect calls, including those identified through analytics, industry traceback requests, or customer complaints.

When potentially illegal or fraudulent traffic is detected, Etex takes appropriate enforcement action based on the circumstances, which may include increased monitoring, engagement with the customer to remediate the issue, traffic blocking, or suspension or termination of service. These measures are applied consistently to protect the network, comply with regulatory obligations, and prevent harm to consumers.

2) Know Your Upstream Provider Procedure *(In accordance with 47 C.F.R. § 64.1200(n)(3))*

Etex exercises due diligence before accepting traffic from any upstream provider to ensure that its network is not used to carry or process illegal or unwanted robocall traffic. Etex maintains an inventory of all carriers from which it directly receives traffic and verifies that each connected upstream provider is accurately identified and listed in the FCC Robocall Mitigation Database (RMD), as required.

As part of its onboarding and ongoing review process, Etex collects and maintains key identifying information for upstream providers, including physical business location, designated contact personnel, state or country of incorporation, federal tax identification number (if applicable), and a description of the provider's business operations and traffic profile.

Etex incorporates robocall mitigation, traceback cooperation, and prohibited traffic provisions into its contractual agreements with upstream providers. These provisions require upstream providers to implement reasonable robocall mitigation practices, cooperate with traceback requests, and take prompt corrective action when illegal or suspicious traffic is identified.

Etex may take appropriate enforcement action, including increased monitoring, traffic blocking, or suspension or termination of service, consistent with its contractual rights and regulatory obligations.

3) Requiring Contractual Provisions

Etex's voice service customers are subject to terms and conditions that forbid customers to use our service for unlawful purposes, such as originating calls that violate laws restricting robocalls or other telemarketing calls. We also preserve our right to suspend or terminate the customer's service immediately for violations of the law.

4) Only Accepting Traffic from Providers Listed in the Robocall Mitigation Database *(In accordance with 47 C.F.R. § 64.6305(g))*

Etex accepts calls directly from domestic, foreign, and gateway voice service providers only if that voice service provider's filing appears in the Robocall Mitigation Database and has not been de-listed pursuant to an enforcement action.

Notwithstanding this policy, Etex does not block emergency calls placed to 911 under any circumstances and makes all reasonable efforts to ensure that calls from public safety answering points and government emergency numbers are not blocked, consistent with applicable FCC public safety safeguards.

5) Mandatory Call Blocking

Etex will block and cease carrying or transmitting illegal traffic when notified of such traffic by FCC and the same for traffic that is found to be substantially similar to the identified traffic on an ongoing basis.

6) Do-Not-Originate (DNO) Compliance *(In accordance with 47 C.F.R. § 64.1200(o))*

Etex blocks calls purporting to originate from numbers included on a reasonable Do-Not-Originate (DNO) list, consistent with 47 C.F.R. § 64.1200(o). Etex maintains and applies its DNO list in accordance with FCC requirements, including confirmation that any unused numbers subject to blocking are verified by the allocatee at the time of blocking. Etex ensures that its DNO list remains reasonable in scope and is not unduly limited.

7) Network Traffic Monitoring and Analysis

Etex utilizes Ribbon's Identity Hub services to monitor and analyze network traffic patterns on an ongoing and real-time basis. Ribbon's cloud-based platform applies reputation scoring and analytics to outgoing call attempts to identify unusual or suspicious calling behavior, including high-volume or repetitive calling patterns, calls originating from unauthorized or invalid sources, and patterns commonly associated with illegal robocalling or nuisance traffic.

Each outgoing call request is evaluated using reputation-based analytics, including fraud and nuisance scoring, and the resulting score informs call treatment decisions. Based on these analytics, calls may be

allowed to proceed normally, rejected with appropriate SIP response codes, or diverted to announcements in accordance with Etex's call treatment policies implemented on its C15 call control server.

The service also provides detailed reporting and alerts identifying suspected illegal robocalls, including calls associated with invalid, unallocated, or Do-Not-Call numbers. When potentially problematic traffic is identified, Etex conducts further investigation and takes appropriate corrective action, which may include working directly with the originating customer to remediate the issue, blocking specific traffic, or suspending or terminating service when warranted.

As part of this process, Etex utilizes a third-party STIR/SHAKEN signing arrangement with Ribbon Communications, under which Etex retains control of attestation decisions and all calls are signed using Etex's own STIR/SHAKEN certificate, as described in the Authenticating Voice Traffic section below.

8) Authenticating Voice Traffic *(In accordance with 47 C.F.R. § 64.6301(a))*

Etex utilizes a third-party signing arrangement with Ribbon Communications to perform the technological act of STIR/SHAKEN call signing, consistent with the FCC's Eighth Report and Order (FCC-24-120). Under this arrangement, Etex retains full responsibility for STIR/SHAKEN compliance and all attestation-level decisions for authenticating caller identification information.

All calls authenticated under this arrangement are signed using Etex's own STIR/SHAKEN certificate associated with Etex's Service Provider Code (SPC) token. Ribbon does not use its own certificate or private key to sign calls. Instead, Ribbon applies the attestation value determined by Etex and uses Etex's certificate solely to generate the PASSporT and SIP Identity header on Etex's behalf.

This third-party signing arrangement is governed by a written agreement specifying the tasks performed by Ribbon and complies with applicable FCC rules requiring that (i) the provider with the STIR/SHAKEN obligation control attestation decisions and (ii) calls be signed using the provider's own certificate.

9) Responding to All Traceback Requests from the Commission, Law Enforcement, and the Industry Traceback Consortium *(In accordance with 47 C.F.R. § 64.6305(a))*

Etex commits to respond fully, within 24 hours, to all traceback requests from the FCC, law enforcement, and the industry traceback consortium. Etex will cooperate with such entities in investigating and stopping any illegal robocallers that use its network to originate, carry or process illegal robocalls.

10) Updating Robocall Mitigation Database Submission and Robocall Mitigation Program *(In accordance with 47 C.F.R. § 64.6305(d)(5))*

Etex will update its submission in the Robocall Mitigation Database within ten (10) business days of any change to the applicable information it must provide in the database, including its Robocall Mitigation Program.