

Fuse 2 Communications, LTD - Robocall Mitigation Plan

Updated February 2026

Overview

Fuse 2 Communications, LLC, ("Fuse 2") is a small voice service provider serving end-user subscribers. This Robocall Mitigation Plan ("Plan") describes the reasonable steps Fuse 2 uses to prevent, detect, and mitigate illegal robocalls for voice traffic that originates on its network, consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301.

Outbound calls originate from subscriber endpoints on Fuse 2's platform and are routed to the public switched telephone network ("PSTN") via an upstream carrier partner; inbound calls are received from Fuse 2's upstream carrier partner and delivered to subscriber endpoints.

This Robocall Mitigation Plan describes Fuse 2's controls, including customer onboarding/KYC, traffic monitoring, and escalation/enforcement.

STIR/SHAKEN Implementation Status

Through network enhancements developed to implement STIR/SHAKEN, Fuse 2 has fully implemented the STIR/SHAKEN caller ID authentication framework across its entire IP-based voice network. All calls that Fuse 2 originates on its network are authenticated and signed in compliance with 47 C.F.R. § 64.6301. Fuse 2 signs outbound calls using in-house developed technology using its own STI-CA issued certificate. Calls are attested only when the calling number is authorized and validated (e.g., from Fuse 2's numbering inventory or supported by customer documentation such as an LOA); unauthorized caller IDs are blocked. While Fuse 2 relies on upstream carrier partners for PSTN interconnection and certain downstream enforcement signals (e.g., spam/analytics feedback and blocking outcomes), Fuse 2 retains responsibility for and control over its call authentication and robocall mitigation program as described herein.

Telephone Number Authorization

A Telephone Number ("TN") based caller identity is the originating phone number included in call signaling used to identify an outbound caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Fuse 2 and/or obtained by Fuse 2 from one of Fuse 2's underlying carriers for use by the subscriber. In most cases, Fuse 2 directly manages the TNs used by its subscribers. Fuse 2 tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Fuse 2's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Fuse 2, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Fuse 2 will attest calls originated with these TNs.

When originating a call, Fuse 2 checks the calling party number against Fuse 2's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Know Your Customer ("KYC")

Accurate identification of an end-user subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. An end-user subscriber is a customer that has a service relationship with Fuse 2 under which Fuse 2 carries and originates outbound calls on the subscriber's behalf and delivers inbound calls to the subscriber.

Fuse 2 uses enhanced detection Call Processing servers by Netaxis Solutions coupled with Oracle and Ribbon SBCS. Customers are blocked from using third party Caller IDs unless they have ported them to Fuse 2 or they can provide evidence they own them. Subscribers are only allowed to use Caller IDs that Fuse 2 provided or vetted.

Fuse 2's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting information such as:

- physical business location;
- contact person(s);
- nature of the customer's business.

Acceptable Use Policy ("AUP")

Fuse 2 maintains an AUP that subscribers must sign before being permitted to use Fuse 2's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable law;
- violating applicable industry accepted guidelines; and
- using Fuse 2's service to engage in or in connection with fraudulent activities.

Fuse 2's contractual terms with subscribers specify that Fuse 2 may take action up to suspension or termination of service for violation of the AUP.

Know Your Upstream Providers

Fuse 2 maintains procedures to identify and validate its upstream voice service provider(s) used for PSTN interconnection and to coordinate mitigation, enforcement, and traceback support as needed. Fuse 2 therefore discloses below its upstream voice service carrier information and will update its RMD filing within the FCC-required timeframe if upstream relationships change.

Fuse 2 has one upstream provider from which it receives voice traffic:

Bandwidth Inc (d/b/a Voxbone)
900 Main Campus Drive
Suite 100
Raleigh NC 27606

Fuse 2 has a master service agreement with its upstream carrier partner and coordinates with the upstream provider as needed to support robocall mitigation, enforcement and traceback cooperation.

Mitigation During Service

Fuse 2 works with its upstream provider to ensure that all subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to those individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features are:

- VoIP-originated calls are signed with subscriber caller ID only after number validation via SMS; and
- requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Analytics for Monitoring Traffic

Fuse 2 works with its upstream provider and to identify behaviors which indicate illegal call activity.

Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Fuse 2 works with its upstream provider to follow defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

Fuse 2 uses the following third-party vendors for call analytics: Netaxis Solutions and VoIP Monitor.

Fuse 2 follows Industry Traceback Group ("ITG") recommended best industry practices and cooperates in traceback and trace forward investigations including responding fully within 24 hours to any traceback requests. Fuse 2 will devote sufficient resources to provide prompt and complete resources to traceback requests.

Fuse 2 works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Fuse 2 by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Fuse 2 contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

For all new and renegotiated Fuse 2 contracts governing the transport of voice calls, Fuse 2 will endeavor to contractually require Fuse 2's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Fuse 2 will implement Do Not Originate requests it receives from the ITG. Fuse 2 has mechanisms to automatically block suspicious calls using internal analytics. If Fuse 2's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Fuse 2 will take appropriate action which may include suspending or terminating the subscriber's use of Fuse 2's network.

Fuse 2 remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities

in investigating and stopping illegal robocallers initiating calls.

Ongoing Efforts

Fuse 2 will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue. In the event of any material change to this Plan, Fuse 2 will republish and file any such update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Point of Contact:

Name: Wayne Mills-Kidal

Title: CTO

Email: wayne.mills-kidals@fuse2.net

Phone: +443339963444

This Plan demonstrates Fuse 2's commitment to protecting consumers, upholding industry standards, and contributing to the elimination of illegal robocalls.