

Business Information
Mitel Cloud Services, Inc.
2160W Broadway Rd, Ste 103,
Mesa AZ 85202

Contact Information

Dave Deutsch
Associate General Counsel, Regulatory & Privacy
4000 Innovation Drive, Kanata, ON K2K 3K1
613-383-1254
dave.deutsch@mitel.com

Overview

The Federal Communications Commission ("FCC" or "Commission") requires that all voice service providers ("VSPs") file a certification in the Robocall Mitigation Database to demonstrate their level of STIR/SHAKEN implementation, describe their Robocall Mitigation Plans ("RMP"), and provide other required information the Commission uses to monitor compliance with its rules. The Commission also requires that VSPs update their RMPs when pertinent corporate or service changes occur.

Purpose

Mitel Cloud Services, Inc. ("Mitel") is a VSP offering Network Services (which includes SIP trunking, long-distance and toll-free services, dedicated data transport solutions (including MPLS and business-grade Internet)) and has implemented reasonable measures to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document reflects the changes in Mitel's business and updates Mitel's RMP.

Robocall Mitigation Plan

Background

Mitel has ended its unified communications as a service (UCaaS) business following the acquisition of MiCloud Connect and Sky (aka ShoreTel Sky) business by RingCentral in June 2024 and the end of life of MiCloud Flex on April 30, 2025.

Currently, Mitel only provides SIP for premise-based solutions via the Network Services offer.

Know Your Customer

As part of the contract process, Mitel requires its customers to provide basic information such as name, address, etc. In addition, Mitel requires customers to update their information when changes occur. At this time, however, no new Mitel Network Services customers or contracts are accepted but existing Mitel customers are allowed to renew their Mitel contracts.

In addition to the above and in order to mitigate illegal robocalls, Mitel's carriers monitor traffic on a per customer and per ANI basis and take action if and when traffic looks problematic, or if Mitel receives complaints.

Mitigation Through Contracts

a. Acceptable Use Policy

Mitel maintains an Acceptable Use Policy ("AUP") that customers must agree to before being permitted to use Mitel's network. Among other things, this AUP prohibits:

- impersonation of any person or misrepresentation of an affiliation with any person;
- violating any applicable local, state, or federal law; and
- using Mitel's service in a manner that can be interpreted as abusive or fraudulent.

Mitel's contractual terms with Network Service customers specify that Mitel may suspend service for violation of the AUP. Repeated suspensions give rise to a termination right.

b. Cloud Services Global Terms of Service (GTOS)

In addition to its AUP, Network Service customers must also agree to Mitel's GTOS before being permitted to use Mitel's network. Section 5.3 of Mitel's GTOS states:

Further, in order to investigate, monitor and limit illegal calls, we may, in compliance with law: (i) perform checks of calls originating from User telephone numbers against known or suspected robocallers and robocall characteristics, and (ii) from time to time, including where required by a regulator, traceback certain User calls to determine the origin. You agree to provide a single point of contact to work with us on Incidents or alleged illegal calls, including tracebacks, and fully cooperate with us (and any regulator) to address same. At our request, you will document any actions taken in response to Incidents or alleged illegal call(s) and provide us with a copy of such documentation.

Know Your Upstream Provider

For upstream providers, Mitel collects basic information such as nature of business, physical business location, contact person(s), and federal tax ID where available. In addition, Mitel ensures that its contracts with its upstream providers (Intermedia) require both parties to ensure compliance with all applicable laws.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the Network Service customer. A Network Service customer is permitted to use a TN as a caller identity if a TN is obtained by Mitel from one of Mitel's underlying carriers for use by the Network Service customer.

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

During Service

Mitel permits Network Service customers to block individual telephone numbers. Network Service customers can obtain details for SIP by contacting support. Network Service customers are not billed for call blocking.

Monitor Traffic with Analytics

Mitel's carriers are actively implementing traffic monitoring on a per customer and per ANI basis looking for a threshold number of short calls within an allotted period which would suggest robocalling and/or fraud. If triggered, Mitel, or its carriers, will initiate the "suspected robocall" review process.

- Mitel's carriers are actively implementing traffic monitoring for anomalies in call duration distribution. If triggered, Mitel, or its carriers, will initiate the "suspected robocall" review process.

Mitel customers have an assigned list of numbers per account. Only numbers assigned to a customer's account can be used to originate calls.

No third-party vendors are involved in deploying Mitel's analytics.

Investigating Suspicious Activity

Mitel is actively implementing the following process for investigating robocall suspicious activity based on its established fraud prevention process:

- Mitel will receive the robocall alert based on Mitel or its carrier's alert mechanism. The Mitel Transport team (Support) will be informed, and an incident ticket will be opened.
- The MiCloud Transport team creates a customer case using Mitel internal ticketing system for tracking purposes and fills out all the required details.
- Support starts validation of the robocall alert or compromised profile.
- Once the telephone number (TN) and respective call details are validated, Support will attempt to contact the Mitel account Decision Maker (DM) to check the legitimacy of the phone calls.
- If the Mitel account DM confirms the legitimacy of the calls, Support closes the case with no further action required and the status of legitimate, or similar call frequency as, robocalls is recorded.
- If unable to get any response from the Mitel account DM by phone or email and there are active suspicious calls, then Support will reach out to the Mitel's Carrier to kill the active calls.
- Support will snip the TN. Further attempts to contact the Mitel account DM will be pursued by Support.
- If after performing the above steps, robocall alerts are still detected. The Mitel Network Team will identify and block the IP address.
- Should Support then determine that a SNIP needs to be reverted because it is confirmed with certainty that robocalls were not actually being made, Support will perform the action and restore service.
- Support will inform the Mitel end customer of the actions taken and then close the customer case.

Blocking

When it is administratively feasible, Mitel will implement in the Do Not Originate requests it receives from the Industry Traceback Group ("ITG"). Mitel and its carriers have mechanisms to block suspicious calls using internal analytics. If Mitel's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Mitel will take appropriate action which may include suspending or terminating the customer's use of Mitel's network. Mitel will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office) to the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto. Mitel will respond to traceback requests within 24 hours of receiving same

After Network Service Has been Used for Illegal Robocalling

Mitel will evaluate suspension or termination of the customer's account if illegal robocalling has been confirmed. Mitel will cooperate with investigative bodies when requested to do so. Requests will be validated similar to subpoenas for Lawful Intercept (CALEA) and documented. Mitel Support will follow process similar to the 'Investigate Suspicious Activity' section above.

Law enforcement, the FCC, or Industry Traceback Group may contact Mitel through the following email address at *Traceback@mitel.com*.

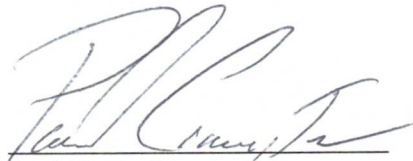
Plan Updates

This plan and industry best practices must evolve in response to the dynamic nature of mitigating illegal robocalling.

In the event of any material change to this plan, Mitel will republish it to applicable employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of the event that effectuates the change.

Last updated: 23 February 2026.

I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that to the best of my knowledge the foregoing is true and correct. Executed on 2/23/2026.

A handwritten signature in black ink, appearing to read 'Paul Ciaramitaro', is written over a horizontal line.

Paul Ciaramitaro
Director, US Taxation
Mitel Cloud Services, Inc.

Certification of Paul Ciaramitaro

I, Paul Ciaramitaro, Director, US Taxation, of Mitel, do hereby certify, under penalty of perjury, the following:

- (1) Mitel's Business name and primary address are as follows:
Mitel Cloud Services, Inc.
2160W Broadway Rd, Ste 103, Mesa AZ 85202
- (2) Mitel has no other business names in use.
- (3) Mitel has not previously used any other business name.
- (4) The following entity owns more than 10% of Mitel: Mitel Networks Inc.
- (5) The following persons are Mitel's directors:
 - Karthik Arurmugam
 - Gregory J. Hiscock
 - Janine Yetter
- (6) None of the persons/entities in items 4-5 above have had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (7) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (8) Mitel's role in the call chain is that of a voice service provider relying on underlying carriers with STIR/SHAKEN implementation obligations, while maintaining its own robocall-mitigation controls for serving end-users.
- (9) Mitel has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (10) Mitel is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (11) Mitel's operator company number is 670J.



Paul Ciaramitaro
Director, US Taxation
Mitel Cloud Services,
Inc.