

VERSATEL LLC
Robocall Mitigation Plan
February 13, 2026

Table of Contents

1. Overview.....2

2. Company Summary.....2

3. Versatel role in the call chain includes:.....2

4. Commitments and Certifications.....2

5. Traceback Requests.....2

6. Know Your Customer (KYC) Process.....3

7. Robocall Mitigation Plan (RMP).....3

8. Certification.....4

Attachment A.....5

Versatel LLC
1503 E 19th Street Edmond, OK 73013

1. Overview

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Plan (“RMP”) details the policies and practices that Versatel LLC (“Versatel”) has established to prevent unlawful robocalls or other unlawful traffic from originating on, terminating to, or routing through Versatel’s voice networks.

1. it has fully implemented the necessary technical and procedural measures to ensure compliance with the FCC’s STIR/SHAKEN framework, and all calls it originates are compliant with § 64.6302(b);
2. it has no type of extension or extensions under § 64.6304;
3. it commits to respond fully and within 24 business hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls;
4. It is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

2. Company Summary

Versatel, a Oklahoma limited liability company and domestic 214 authority holder, provides interstate interexchange service primarily to end users throughout the United States.

Entities Covered by Certification:

The following entity is subject to robocall mitigation policies and procedures described in this document:

- Versatel, LLC

Versatel OCNs

- 962J

3. Versatel role in the call chain includes:

- Voice Service Provider with STIR/SHAKEN implementation
- Gateway Provider with STIR/SHAKEN implementation
- Non-Gateway Intermediate Provider with a STIR/SHAKEN implementation

4. Commitments and Certifications

Versatel is fully committed to mitigating and eliminating illegal robocalling activity. Versatel has an ongoing commitment to help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns of prohibited robocalls, removing bad actors from the Versatel network, and collaborating with other providers and regulatory agencies in combatting fraudulent voice activity.

5. Traceback Requests

Versatel commits to responding to all traceback requests from the FCC, law enforcement, the industry traceback consortium (ITG), and other regulatory entities within 24 business hours of receipt of such request. Upon receipt of a traceback request, Versatel promptly conducts an internal investigation to determine the source of suspected illegal traffic. The findings are reported back through the official traceback portal.

- **Client Notification:** Versatel promptly notifies the customer responsible for the illegal traffic, requesting immediate corrective action and proof of resolution.
- **Service Suspension and Termination:** If the customer fails to respond or resolve the issue to Versatel’s satisfaction within 2 days, Versatel will issue a final warning requiring remediation

within 24 hours before suspending or terminating the customer's traffic from conveying through the Versatel network.

- **Continuous Review:** On a regular basis Versatel performs regular reviews of traceback reports to identify patterns. Any upstream customer with three or more traceback incidents within 30 days is flagged for executive review, with potential service termination.
- Versatel also promptly responds to inquiries from law enforcement and regulators, including the FCC, Federal Trade Commission ("FTC") or state attorneys general seeking traceback or similar information. The designated employee responsible for addressing traceback inquiries is as follows:

Contact Name: Amy Lasitter
 Contact Department: Traffic Fraud Department
 Contact Title: Senior Fraud Prevention Specialist
 Contact Street: 603 Munger Ave Suite 300
 Contact City: Dallas
 Contact State and Zip Code: TX 75202
 Contact Telephone Number: (469) 587-7134
 Contact Email: Amy.Lasitter@46labs.com; with cc to Legal@46labs.com

6. Know Your Customer (KYC) Process

Consistent with 47 C.F.R. § 64.1200(n)(3), the Know Your Customer ("KYC") principles is at the forefront of Versatel's business practices. A large majority of Versatel's traffic and services are supported in its capacity as an Intermediate Service Provider without direct end-user relationships. Similarly, Versatel operates in the role of an International Gateway Provider. Versatel has a stringent mandatory on-board screening process designed to proactively identify and prevent prospective entities that may engage in illegal robocalling or other fraudulent activity from becoming a customer of Versatel through its KYC process. Additionally, Versatel confirms that a prospective customer is registered in the FCC's robocall mitigation database. The KYC form can be found as Attachment A at the end of this document.

7. Robocall Mitigation Plan (RMP)

Versatel has implemented a comprehensive RMP using data systems for analytics and reviews to identify illegal robocalling in addition to a KYC requirement to access the Versatel network. The key elements of the RMP are as follows:

- When traffic analysis indicates the presence of illegal robocalling or other fraudulent traffic, Versatel may follow certain procedures on investigating such customers. The procedures established may 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 strange behavior; contacting the customer to understand his or her particular use case and validate that the activity belongs to that customer.
- Versatel fully implemented the STIR/SHAKEN framework for all IP-based traffic.
- Pursuant to FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (n)-(o), Versatel blocks calls that purport to originate from telephone numbers included on a reasonable Do-Not-Originate ("DNO") list. In addition, consistent with applicable FCC robocall mitigation and call-blocking requirements, Versatel employs network-based call blocking measures, including the use of SIP response code 603 (Decline / Network Blocked), where appropriate, to reject calls that are highly likely to be illegal, spoofed, or otherwise non-compliant.

- Versatel has contractual rights that allow it to terminate customers that violate applicable law, including violations of the Telephone Consumer Protection Act. When appropriate, Versatel enforces these rights. Versatel also terminates accounts if it discovers that any of the entities or individuals associated with a customer account have been named by the FCC or the FTC as an illegal robocaller or have failed to respond to traceback requests.
- Consistent with 47 CFR §64.6305(g)(2), Versatel confirms to continue to remove any telecommunications carriers from its network that do not have a RMP on file in the Robocall Mitigation Database (RMD). Similarly, upon notice from the FCC, Versatel promptly removes telecommunication carriers from its network where the carrier has failed to implement an effective RMP.
- Versatel will continue to monitor the FCC publicly released listings of voice service providers who have triggered requests and promptly block any traffic when notified by the FCC.
- In accordance with 47 C.F.R § 64.6305(e)(1), Versatel only accepts calls directly from a domestic Voice Service Provider only if that Voice Provider's filing appears in the RMD and that filing has not been delisted pursuant to an enforcement action.
- Versatel sets predefined Call Per Second (CPS) and channel limits for customers, ensuring that no customer can process unlimited simultaneous calls.
- All outbound traffic is authenticated via SIP Registration or authorized IP addresses before termination.
- The Versatel system continuously monitors key call statistics (e.g., Call Completion Ratio (CCR), and Average Call Duration (ACD)) to detect suspicious traffic patterns. If anomalous behavior is detected, the system can automatically block calls based on ANI.
- Originating and termination numbers are profiled by traffic analytics engine for abnormal behavior including but not limited to: High Volume / Short Duration Traffic, Calls to Unallocated Numbers, and Calls with excessive cancels.

8. Certification

I certify, under penalty of perjury, that the above Robocall Mitigation Plan is true and accurate, and that Versatel LLC complies with all relevant FCC regulations regarding robocall mitigation.

Name: Ali Mumtaz

Signature: 

Title: Chief Technical Officer

Date: Feb 13 2026 05:24 CET

Attachment A

**46 LABS AND ITS SUBSIDIARIES
(VERSATEL LLC, IMPACT TELECOM LLC, HYPECUBE NETWORKS LLC)
KNOW YOUR CUSTOMER (KYC) QUESTIONNAIRE**

Company Information		
1	Legal Name of Business/Company .	Click or tap here to enter text.
2	All business and trade names, fictitious names, and DBAs, as well as names of any predecessor entities.	Click or tap here to enter text.
3	Company Type (C-Corp, S-Corp, LLC, Sole Proprietorship)	Click or tap here to enter text.
4	Principal legal name of the owner(s) of company. If a C-corp. provide name of principal shareholder	Click or tap here to enter text.
5	Parent Company Name (if any)	Click or tap here to enter text.
6	Headquarters Street Address, City, State Zip	Click or tap here to enter text.
7	State/Country and Year of Incorporation	Click or tap here to enter text.
8	Information about managers (if different than principal(s), controlling person(s), or person(s) with a majority ownership in the entity). Provide name(s) of General Manager, Chief Executive(s) and head of Operations.	Click or tap here to enter text.
9	Has the business/company, its predecessor(s), its parent/affiliate(s), or its principal(s)/controlling person(s) ever been subject to an adverse judgment arising out of a civil lawsuit relating to the use of telecommunications networks or been the subject of any law enforcement action or investigation by any local, state, or federal agency? (Yes/No). If yes, please describe adverse judgment/action, including case/docket	Click or tap here to enter text.

	numbers.	
10	Background Check: Do you consent to a background check on your business and/or the principal owners/managers? This may include verification of credit history.	Click or tap here to enter text.
11	Website Address(s) What other domains has your company used in the past? List all of them and the dates of their usage.	Click or tap here to enter text.
12	Social Media Handles (LinkedIn, X, Facebook, etc.)	Click or tap here to enter text.
13	Compliance Contact: Full Legal Name, Email and Phone Number	Click or tap here to enter text.
14	Operations/Network Contact Full Legal Name, Email and Phone Number (to address traffic complaints).	Click or tap here to enter text.
15	FCC Registration Number (FRN) If no FRN, explain why.	Click or tap here to enter text.
16	Operating Company Number (OCN) If no OCN, explain why.	Click or tap here to enter text.
17	Foreign ownership (yes/no)	Click or tap here to enter text.
18	FCC 214 registration number	Click or tap here to enter text.
19	499 Filer ID If no 499 Filer ID, explain why.	Click or tap here to enter text.
Customer Base and Traffic Type		
20	Type of Business (e.g., VoIP, wholesale, retail, wireless, non-communications, etc.)	Click or tap here to enter text.
21	Type of voice services provided (e.g., local, long distance, toll-free, inbound only, outbound only, etc.)	Click or tap here to enter text.
22	Describe type of customers you serve (e.g., wholesale, conference calling, domestic/international, enterprise, wireless carriers, etc.)	Click or tap here to enter text.
23	Do you engage in telemarketing (Yes/No)? If yes: (a) Do you have policy and process in place to ensure that none of your telephone calls will be placed to persons registered on the DNC Registry or any analogous state registry, and that you will adhere in all other respects to the telemarketing restrictions adopted by the FCC, FTC, and states (Yes/No)? (b) Will prerecorded/artificial	Click or tap here to enter text.

	messages and/or an automatic telephone dialing system be used, and if so, can you confirm you will obtain evidence of prior express written consent from each person called (Yes/No)?	
24	Do you originate or transmit high-volume, short-duration voice traffic? (Yes/No)? If yes: (a) what is the nature of this traffic? (b) Has this traffic been the subject of any inquiries through the Industry Traceback Group or any investigations or enforcement actions by any federal, state, or local body?	Click or tap here to enter text.
25	Do you generate auto-dialed traffic? (Yes/No) If yes: describe whether auto-dialed traffic is specific to United States NANP numbers using U.S. NANP origination numbers, and whether traffic originates from domestic U.S. or international.	Click or tap here to enter text.
26	Have you, or any of the controlling person(s) of the entity, ever had an adverse judgment in a civil lawsuit alleging claims under the Federal Trade Commission Telemarketing Sales Rule (TSR), the TCPA, or any other lawsuit regarding robocalls, automated dialing, calls to the DNC Registry or any state do not call registry, spoofed caller ID numbers, or otherwise unlawful telemarketing or solicitations? (Yes/No)	Click or tap here to enter text.
27	Are you a Gateway Provider (a provider that is the entry point for foreign calls into the United States)? (Yes/No) If yes, do you certify to comply with Gateway Provider requirements, such as responding to traceback requests within 24 hours, blocking mandates, and “know” the provider immediately upstream from the gateway provider? (Yes/No)	Click or tap here to enter text.
28	Have you implemented STIR/SHAKEN in your network? (Yes or No) If no, please explain why, including a reference to the extension(s) received under 47 CFR §64.6304.	Click or tap here to enter text.
29	Have you been blocked from any other voice service provider's network after being determined to be a "bad- actor upstream voice service provider" with accordance to a notice from the FCC? (Yes or No)	Click or tap here to enter text.
Fraudulent Traffic Mitigation		
30	Are you a member of the US Telecom Industry Traceback Group? (Yes/No)	Click or tap here to enter text.
31	Do you participate in US Telecom Industry Tracebacks? (Yes or No) If yes, provide name, email, phone number of contact responsible for tracebacks.	Click or tap here to enter text.
32	Have you been determined by the US Telecom Industry Traceback Group to be a "Non-Cooperative Voice Service Provider"? (Yes/No)	Click or tap here to enter text.
33	Provide the number of tracebacks you have received in last 3 months and 6 months? Have any of these tracebacks resulted in a finding that	Click or tap here to enter text.

	fraudulent/illegal traffic originated from or transited through your network?	
34	Are you registered in the Robocall Mitigation Database (RMD)? (Yes/No) If yes: • Provide RMD registration number.	Click or tap here to enter text.
35	Do you have a policy and a process in place ensuring that you do not originate or transmit fraudulent or otherwise illegal voice traffic, including a procedure for blocking such traffic when notified by the FCC, the FTC, state attorneys general, other law enforcement bodies, and/or the Industry Traceback Group? (Yes/No)	Click or tap here to enter text.
36	Are you a Gateway Provider (a provider that is the entry point for foreign calls into the United States)? (Yes/No) If yes, do you certify to comply with Gateway Provider requirements, such as responding to traceback requests within 24 hours, blocking mandates, and “know” the provider immediately upstream from the gateway provider? (Yes/No)	Click or tap here to enter text.

The undersigned certifies that s/he is an officer of the Company. The undersigned affirms and certifies that all information and answers to questions herein are complete, true, and correct to the best of signatory’s knowledge and belief. The undersigned confirms that blocking of customer traffic may occur as a result of the customer failing to provide notice of material updates to its KYC certification, demonstrated illegal/fraudulent traffic, customer delisting in the Robocall Mitigation Database, or otherwise required by regulatory or law enforcement agencies.

I verify that I am authorized to legally bind the Company by my signature.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Business Address: Click or tap here to enter text.

Email: Click or tap here to enter text.

Telephone Number: Click or tap here to enter text.

Date: Click or tap here to enter text.