

VERCOM SYSTEMS, INC.
Robocall Mitigation Plan
V.3.0 February 2026

STIR/SHAKEN IMPLEMENTATION

VerCom Systems, Inc. ("VerCom") located at 410 Fame Rd, Dayton Ohio 45449, is an interconnected VOIP Provider of SIP Services and does not have access to any switching facilities and solely relies on its SIP Provider (who interfaces with the telecom switching infrastructure) for providing access to the Telecom Network. VerCom has not been prohibited from filing a certification in the Robocall Mitigation Database. VerCom does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

ROBOCALL MITIGATION

Background

The FCC Order lists the following affirmative obligations for interconnected voice service providers: (1) Respond to traceback requests from the Commission, Civil and Criminal Law Enforcement, or the Industry Traceback Consortium; (2) Take steps to effectively mitigate illegal traffic when it receives notification of such traffic from the Commission through its enforcement bureau; (3) implement affirmative, effective measures to prevent, new and current customers from originating illegal calls; (4) implement STIR/SHAKEN when applicable; and (5) implement Know your Upstream Provider

1. Traceback:

VerCom maintains detailed call records for all call traffic from the PBX Switch for thirty (30) days, allowing VerCom to track each instance of a call's origination and destination. VerCom also records call history perpetually in the system's Call Detail Reporting Database, which allows VerCom to see historically any calls that were made through the system and what source and destination channels were involved in the calling process. The Upstream Carrier providing access to the Telecom Network, also maintains call detail records to assist with any TraceBack requests. VerCom responds within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. VerCom cooperates fully with such entities in investigating and stopping any illegal robocallers from using our service to originate, or process illegal robocalls.

Traceback Contact Information

Robocall Mitigation Plan for VerCom Systems, Inc.

Name	Title	Contact Information
Ronald Hartmann	Director of Technical Services	Ph: 937-353-2004 Email: rhartmann@vercomsystems.com

2. Take Steps to Mitigate Illegal Traffic

The IPlex PBX Solution automatically blocks any calling devices that do not belong to the customers' network or attempts to connect from the customers' network and fails to authenticate. VerCom actively blocks any calls attempting to reach a destination outside of the NANP calling plan. Outbound calls are checked to ensure that the out pulsed Caller ID is one that the customer has a legal right to use. All other calls are dropped. VerCom contracts inform its customers that any suspected illegal calling, or attempted calling, could result in outbound services (except calling to emergency numbers) being suspended during the investigation of possible illegal calling, and could be terminated if the investigation reveals that the client actively engaged in illegal calling.

VerCom uses call analytics software provided by TransNexus to monitor voice traffic in real-time to prevent the origination or transit of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we attempt to process calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list, resulting in the blocking of the call.

Do Not Originate (DNO) Screening:

VerCom utilizes TransNexus for Do Not Originate (DNO) lookups and enforcement on both ingress and egress call traffic. DNO screening is applied to calls received from upstream providers for termination (ingress) and to calls originated by VerCom customers and delivered to upstream providers (egress). If the calling number is identified as invalid, unallocated, or listed on a Do Not Originate list, the call is blocked and logged for investigation.

VerCom immediately investigates any identified suspicious calls to determine if the caller, customer, or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

3. Affirmative, Effective Measures to prevent origination of illegal calls

Know Your Customer:

VerCom follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group. VerCom has a direct relationship with all its clients and collects the following information during customer engagements: (i) W9 Form (and/or) EIN Verification Number (and/or) Vendors License, (ii) a copy of the former telephone bill, (iii) business address, (iv) nature of the business, (v) contact name of an officer of the client.

VerCom does not permit automated outbound calling, or connection of automated calling equipment, and confirms with the client that they have no need for, nor do they have intentions to perform any automated calling. Our contractual provisions with customers prohibit them from initiating illegal robocalls. If VerCom finds a customer initiating suspicious robocalls, they are given a warning to stop. If such traffic continues, then their service is terminated.

Telephone Number Validation:

VerCom obtains its telephone numbers through a 3rd Party SIP Trunk Provider, who also manages all phone number procurements and porting. As a part of the porting request, VerCom provides the SIP Trunk Carrier with an LOA from the customer and a current phone bill (from the incumbent provider). The phone bill must include a listing of all phone numbers that the customer would like to have ported to VerCom's services.

Network Monitoring:

VerCom monitors and inspects call traffic to prevent the origination or transit of illegal robocalls and spoofed calling activity. Monitoring includes authentication and authorization controls, validation of calling and called numbers, and the use of TransNexus analytics and DNO screening.

Outbound / Egress Monitoring:

Outbound calls are inspected to ensure that:

1. The attempt to make a call is from an authenticated device that resides on the customer's network.
2. The attempted call has a destination that resides in the NANP calling plan.

3. The attempted call has a Caller ID that the customer has a legal right to use, is not invalid, is not unallocated, and is not on a Do Not Originate list (as determined by TransNexus DNO and reputation analytics).
4. The attempted call has a valid destination number.

Call Blocking:

If VerCom determines that a call is illegal it is dropped and the reason for blocking the number is logged. These logs allow VerCom to identify calling patterns that may indicate fraudulent patterns. Logs are inspected for a large number of calls in a short period of time that result in short durations. These calls are then flagged as being suspicious and further investigation is performed.

VerCom is a pure reseller of SIP Services and does not have access to any switching facilities. VerCom's relationship with its SIP Provider ensures that incoming calls are actively blocked for certain calls before they reach our endpoint, as authorized by the FCC to combat illegal robocalls as follows:

1. - Calls from numbers on the Do-Not-Originate list
2. - Calls from unassigned numbers
3. - Calls from invalid numbers
4. - Calls from numbers not allocated to any provider

4. STIR/SHAKEN

VerCom is registered with the STI-PA using OCN 903J. VerCom has its own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that is used when authenticating calls that we originate. VerCom has implemented a STIR/SHAKEN solution supplied by TransNexus.

5. Know Your Upstream Provider:

VerCom is an Interconnected VoIP Provider without network facilities. As a reseller of SIP Service, we have a vetting and review process for providers that we interact with, that is, providers that send us voice traffic that we terminate, or that we send voice traffic to for connection to the telecom network. VerCom requires that these providers have an entry in the RMD, have a vetting process for their customers and upstream providers, and have a Prevention, Detection, and Mitigation operational procedures in place. These providers drop any calls that reach their network, from providers that are not listed in the RMD as permitted or directed by the FCC, are subsequently dropped from the RMD, or when advised by the FCC to Drop Traffic prior to sending them to our Endpoints for termination.

6. Acceptable Use Policy

VerCom has prepared an Acceptable Use Policy ("Policy") as a guide for its customers to understand the intended and permissible uses of our service, and to prevent exploitation, fraud, and abuse of our unlimited calling plans and features. This Policy is applicable to all our services and can be found at the following link: <https://www.vercomsystems.com/acceptable-use-policy>