

Robocall Mitigation Plan
For Infotel Systems, Inc.
FRN 0025466137
Adopted 5-1-2021, Updated 2-22-2026

Infotel Systems, Inc. is a small VoIP service provider with less than 100,000 business (no consumer) subscribers. We have implemented the following Robocall Mitigation Plan for compliance with the TRACED Act and STIR/SHAKEN (FCC 20-136). Updated to FC 24-135.

As of the date of this filing, Infotel Systems, Inc. has no ongoing investigations related to suspected unlawful robocalling or spoofing.

Infotel Systems reviews and updates its Robocall Mitigation Plan at least annually.

Robocall Mitigation Database	1. We have established a CORES account with the FCC for inclusion on the FCC database. 2. We have established the role of Compliance Officer to keep registration up to date and be the liaison with law enforcement and upstream carriers. 3. We have verified and recertified our filing in the Robocall Mitigation Database
OCN Company Code: 736K	We have obtained an OCN from NECA and have an STI-Certificate on file with an Approved Certification Authority
Update Alerts	1. We have a relationship with Marashlian and Donahue, PLLC for compliance issues. 2. They routinely send updates to us to assist in compliance with any changes required by the FCC

Before Service is established for a new customer

Compliance Requirement	Steps to Ensure Compliance
Measures to prevent new and renewing customers from originating illegal robocalls	Only numbers assigned to the customer may be used for outbound CID. Moving a VoIP phone to another IP network will disable the phone.
Know your Customer (KYC)	We do an on-site install to 99% of all customer sites. We do not sell to downstream Communication Service Providers
Customer acknowledgement of our compliance to Traceback Requests	Such verbiage has been added to all sales contracts and installation agreements (terms and conditions).
Customer acknowledgement that they are prohibited from instigating unauthorized Robocalling	Such verbiage has been added to all sales contracts and installation agreements (terms and conditions).

During Service

Compliance Requirement	Steps to Ensure Compliance
Customer based call blocking	1. Call blocking is part of our feature set and the method is in the first day training guide. 2. Additionally, we offer our customers a spam filter feature for inbound calls to them from the public switched telephone network. The spam filter route calls to a desired destination such as voicemail using program logic similar to a cellular carrier's Call Filter app for a smart phone.
Prevent End Users from Robo Call Origination and Robo Call Termination	1. We have fraud control limits within our network to prevent customers from originating international calls and with our upstream carriers to limit long distance and international calls from our IP addresses through their network. 2. We have limits for maximum simultaneous calls per account, maximum calls per account and max call invites per second. 3. We have alerting sensors that monitor and alert on high (voice process) CPU count that could indicate robocalling. 4. We have access to Call Detail Records from the end point origination/termination and from our upstream carrier to investigate abnormal calling patterns. 5. Traffic monitoring alerts and mitigation thresholds are reviewed periodically to ensure effectiveness.
Third Party Call Analytic Systems	We do not use third party call analytic systems, thus do not pass any charges for such to customer bills.

After Service Has Been Used for Illegal Robocalling

Compliance Requirement	Steps to Ensure Compliance
Investigation of Alerts received from our systems.	1. Our SBC sends our service system a report on suspected activity. 2. We don't switch any traffic that is not sourced by our customer's end point. "Traceback" is a trivial matter as a traceback would only be to a phone. Identification is easy. 3. Upon an alert, we will then investigate all calls for a 24-hour period for the customer. We will simply warn the customer and a second occurrence will result in service suspension for the offending endpoint. Inbound calls and outbound 911 calls will be allowed. 4. Mitigation procedures will be enhanced if such events occur. So far, zero events have occurred.
Traceback requests by law enforcement, the FCC, or the Industry Traceback Group	1. All requests will be researched and investigated with 24 hours of such request. (FCC 23-18) 2. Any request with a specific time, call duration and destination number will be deemed sufficient proof that passes any CPNI test. Once these 3 data points are collected from our web form, we will trace the call in our network and respond that (first occurrence) customer was warned, 2nd occurrence, customer's service will be suspended for the offending endpoint. 3. We have a single point of contact, our current utility manager, an experienced 9-year employee. 4. We have agreements in place with our upstream wholesale provider to assist in any inbound or outbound traceback required for our end user. 5. We have an SSI on file in compliance with CALEA and TCPA and review and updated periodically. 6. Infotel Systems will block traffic when it is determined to be illegal or when directed by law enforcement or traceback authorities

Federal, State, and Local authorities	Our Compliance Manager is the single point-of-contact when working with Federal, State, and local authorities.
---------------------------------------	--

ENHANCED ROBOCALL MITIGATION REQUIREMENTS (Per FCC 23-18)

We are signing our calls with our own STIR/SHAKEN certificate.

The url for its store is available on demand from any fcc.gov email address.

We have validated our full STIR/SHAKEN compliance using an industry test number 920-666-1392. The service names us as the certificate holder by saying “The call was certified by Infotel Systems, Inc.” Full A-level attestation is applied only when Infotel has a direct authenticated relationship with the end user and has verified the right to use the calling number.

The service also grades our call to the service with attestation = “A”.

As a control, we can create calls to the 920-666-1392 service on other retail service routes such as a test Comcast line. We deliberately spoof a number not assigned on the facility.

The system states “This call was certified by Comcast” The service properly assigns the test call to the service with an attestation grade = “B”.