



ONTARIO SYSTEMS/FINVI/Fonative

Robocall Mitigation Plan

V 5.0

1 Robocall Mitigation Plan

Plan Title:	Robocall Mitigation Plan
Author:	Rozanne Andersen
Owner:	Angela Erwin
Endorsed By:	Risk/Legal Department
Contact:	Angela.Erwin@finvi.com , (765) 744-0324
Policy Type:	Compliance
Version:	5.0
Operating Company Number (OCN):	684J
Last Update:	5/5/2021, 03/19/2022, 02/21/2022, 2/18/2026
Next Review:	1-year or until superseded

2 Document Control

2.1 Document Title: Robocall Mitigation Plan

2.2 Version History

Version	Date	Author	Change Summary
1.0	5/5/2021	Rip Harris	Initial Version
2.0	6/18/2021	Rip Harris	New contact names
3.0	3/19/2022	Rozanne Andersen	New company name and new contact names
4.0	4/21/2024	Rozanne Andersen	Feb 26, 2024 FCC 6 th and 7 th Order Requirements
5.0	2/18/2026	Angela Erwin	New contact names. Updated description of Sansay interactions.

2.3 Approvals

Name	Title	Date	Version
Rozanne Andersen	Chief Compliance Officer	4/21/2024	1180
Angela Erwin	VP, Risk & Compliance	2/18/2026	

3 Overview

As part of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Federal Communications Commission (FCC/Commission) adopted rules requiring voice service providers to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks.

The FCC requires that all providers certify in the [Robocall Mitigation Database](#) that they have fully implemented STIR/SHAKEN or have instituted a Robocall Mitigation program to ensure that they are not originating illegal robocalls.

The Commission requires voice service providers to develop a Robocall Mitigation plan that:

- details the reasonable steps taken to avoid originating illegal robocalls
- demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls
- is filed in the Robocall Mitigation Database.

The Commission stated that a robocall mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

4 Purpose

Ontario Systems and Fonative are Voice Service Providers dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network following FCC regulations.

This document defines the Robocall Mitigation plan for Ontario Systems and its affiliated companies. Ontario Systems LLC is a Massachusetts corporation doing business as Finvi and is the parent company of Fonative (previously called Ampersand).

5 Acceptable Use Policy

Ontario maintains an Acceptable Use Policy (AUP) that subscribers must sign before being permitted to use Ontario’s network. Amongst other things, this 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 local, state, or federal law;
- violating applicable industry accepted guidelines such as the CTIA, the Mobile Marketing Association, applicable telecommunications industry groups, or any other accepted industry associations; and
- using the Ontario service to engage in or in connection with fraudulent activities

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

6 “Know Your Customer” [KYC]

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Ontario in which we transit, originate and/or terminate calls on behalf of the subscriber.

Ontario's KYC program requires a signed contract with our subscriber. Prior to signing a contract, Ontario confirms a subscriber's identity by vetting a subscriber directly or by using a third-party vetting service. The vetting process includes collecting information such as:

- physical business location,
- contact person(s),
- state or country of incorporation,
- federal tax ID,
- the nature of the customer's business.

7 Telephone Number Authorization

For the purposes of this plan a Telephone Number (TN)-based caller identity is defined as the originating phone number included in call signaling used to identify the caller for call screening purposes that is uniquely associated with a subscriber. A TN used for caller identity may or may not be associated with the subscriber's account with the responsible party.

A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Ontario and/or obtained by Ontario from one of Ontario's underlying carriers for use by the subscriber. In most cases, Ontario directly manages TNs used by its subscribers. Ontario tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Ontario'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 Ontario, then TN validation is necessary. If a subscriber or a subscriber's End-User can provide a valid Letter of Authorization (LOA) that they are the authorized user of such TNs, Ontario will attest calls originated with these TNs.

When originating a call, Ontario checks the calling party number (also called the ANI) against Ontario's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

8 Monitoring

Ontario has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems alert on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal robocalls and attempts at illegal call spoofing.

If Ontario detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network we will seek to identify the party that is using our network to originate, route, or terminate these calls and take appropriate action.

Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate, route, or terminate calls on our network.

9 Investigation of Suspicious Activity and Traceback

Ontario follows Information Technology Governance (ITG)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Ontario will dedicate sufficient resources to provide prompt and complete responses to traceback requests.

Ontario will investigate suspicious activity found by its monitoring systems or reported to Ontario by consumers or third parties. The investigation could potentially result in opening a traceback request or with Ontario contacting a subscriber to correct improper use of the platform, or, if the subscriber or subscriber's End-User does not respond or comply, to block their use of the platform.

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

10 Blocking

When it is administratively feasible, Ontario will implement Do Not Originate (DNO) requests it receives from the ITG.

If Ontario's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Ontario will take appropriate action which may include suspending or terminating the subscriber's or End-User's use of Ontario's network.

11 Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Ontario will monitor industry best practices and continuously improve our internal processes to ensure this plan and our systems adapt to this ever-changing issue.

In the event of any material change to this Plan, Ontario will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within 10 days of such update.

Legal notices may supersede certain provisions of these terms or terms located in other Ontario documents.

12 STIR/SHAKEN

Ontario fully implemented STIR/SHAKEN with its 2022.5 release. Ontario is integrated with a service from Sansay which allows Ontario/Finvi/Fonative to sign our calls.

13 Definitions

Attestation – In the context of SHAKEN, the attestation of a call is represented by an “attest” claim allowing the OSP that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call. This includes the known validity of the TN-based caller identity.

Customer – Typically a service provider's subscriber, which may or not be the ultimate End-User of the telecommunications service.

End-User – The entity ultimately consuming the VoIP-based telecommunications service and may include the End-User's device used for placing the call.

Originating Service Provider (OSP) – The service provider that handles the outgoing calls from a customer at the point at which they are entering the public network. The OSP performs the STIR/SHAKEN Authentication function. The OSP may also serve in the role as TNSP, Resp Org, TN reseller and other roles.

Resp Org – A Responsible Organization is an entity authorized by the FCC to assign tollfree numbers to stCustomers. A Resp Org may also be a service provider, a TN Reseller as well as act in other roles.

Subscriber -- A subscriber is an entity that has a business relationship with a VSP in which the VSP transits, originates and/or terminates calls on behalf of the subscriber

Telephone Identity – An identifier associated with the originator or a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

Telephone Number Caller Identity – Represents the telephone number used in a telephone call that is uniquely associated with a subscriber.

Telephone Number Service Provider (TNSP) – Service Provider (SP) that has been formally assigned TNs by the national numbering authority (e.g., NANPA). A TNSP may assign a subset of its TNs to a business entity (i.e., TN Assignee), to be used as Caller Identification (ID) for calls originated by the business entity. TNSPs can also serve in the role as OSP or TSP.

Terminating Service Provider (TSP) – The VSP of the called party. The TSP performs the STIR/SHAKEN Verification function.

Third-Party Vetting Service – A service provided to a VSP by a third party for the purpose of vetting potential and current subscribers.

Third-Party TN Validation Service – A service provided to a VSP by a third party for the purpose of confirming the right-to-use of TNs for potential and current subscribers.

TN-based Caller Identity – The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases, this may be the Calling Line Identification or Public User Identity. In other cases, this may be a TN-based caller identity that is not associated directly with the calling line or account of the subscriber.

TN Right-to-Use/Authorization – When a party is appropriately assigned a TN, this is the right-to-use that TN; the assignment confers the right to the use of the numbering resource.

TN Validation – A process by which an indirect End-User's authorization to use a telephone number or set of telephone numbers is established and the process of providing that information to the VSP originating the call onto the telephone network through the use of existing and upcoming standardized secure mechanisms. TN Validation can be performed at the time the right-to-use of telephone numbers is established or throughout the life of the contract.

Value-added Service Provider (VASP) – Generally, a third-party provider supporting value-added services, for example including applications beyond the core voice calling services offered by a traditional VSP. In this document, it is used as a general term for VoIP and VoIP application providers that offer voice services without having direct interconnection with other VSPs utilizing wholesale providers for call origination and termination.

Vetting – A process by which a customer's identity and operational legitimacy is confirmed by their service provider. Confirmation can be performed at the time service is established (initial confirmation of identity) or throughout the life of the service subscription or contract (ongoing confirmation such as evaluation of roboscores or traffic patterns indicative of abusive robocalling). TNs are not part of the vetting process; TNs are covered by the TN Validation process.

Voice Service Provider (VSP) – The service provider whose network is interconnected to other service providers to both originate and terminate calls across the telephone network. The VSP is responsible for performing both STIR/SHAKEN Attestation functions when acting as the OSP and STIR/SHAKEN Verification functions when acting as the Telephone Service Provider (TSP).