



Robocall Mitigation Plan

2026

© 2023 Civicom. All Rights Reserved
+1 2036181811 | P.O. Box 4689, Greenwich, CT 06831
www.civi.com

Version Control:

Version	Purpose/Change	Author	Approver	Date
1.0	Initial draft / Template Creation	EL.Uy <i>Contracts & Compliance Associate</i>	M. Pascua <i>Information Security and Compliance Officer</i>	18 June 2025
2.0	Updated the target completion of STIR/SHAKEN implementation	EL.Uy <i>Contracts & Compliance Associate</i>	M. Pascua <i>Information Security and Compliance Officer</i>	25 February 2026

1. Company Information

Legal Entity Name: Civicom, Inc.

Registered Mailing Address: P.O. Box 4689, Greenwich, CT 06831

Contact Name: Steven Knight

Title: Lead Network & Security Engineer

Email: steven.knight@civi.com

Phone: +1 2036181811

FCC Registration Number (FRN): 0018-2215-15

2. Certification Statement

Civicom certifies that it has implemented a robocall mitigation program pursuant to the FCC requirements for all voice traffic that originates on its network, and will fully cooperate with the Commission, law enforcement, and the Industry Traceback Group (ITG).

At present, Civicom is not yet signing calls via STIR/SHAKEN *but is actively working* toward implementation, as outlined in Section 4.

3. Call Origination Overview

Civicom provides VoIP-based communication services. Depending on the service type:

- **PBX Environment:** Employees place outbound calls through the PSTN using SIP carriers that are connected to the telephony network.
- **Conferencing Services:** Calls originate from Civicom's conferencing servers, are transmitted to our carriers, and are then routed through the PSTN.
- **ScribePT Services:** Certain ScribePT servers initiate outbound calls to the PSTN via carriers with whom Civicom maintains an established relationship.

In all cases, calls originate on Civicom-managed equipment or servers and are transmitted to a carrier with established PSTN connectivity.

Types of Calls: Domestic and international calls, including business voice communications.

Jurisdictions Served: United States and applicable international jurisdictions.

4. STIR/SHAKEN Implementation Plan

4.1. Current Practice

Civicom currently does not sign outbound calls using STIR/SHAKEN. All calls are delivered via SIP trunking partners without direct STIR/SHAKEN authentication.

4.2. Planned Implementation:

Civicom is actively in the process of meeting the STIR/SHAKEN requirements. The company has begun filing for a 499-A Filer ID and Operating Company Number (OCN) from NECA. Once those are

secured, we will request an SPC Token from the STI-GA and procure a STIR/SHAKEN certificate to begin call signing. Once issued:

- Calls originating from platforms that support signing (e.g., conferencing and ScribePT SIP servers) will be signed directly.
- For the PBX environment, Civicom will use delegated signing, authorizing our carrier Bandwidth to sign calls on our behalf using Civicom's own STIR/SHAKEN certificate.

4.3. Timeline:

- **Estimated implementation:** May 2026

Additional controls and ongoing mitigation efforts are detailed in the following section: **Robocall Mitigation Program Components.**

5. Robocall Mitigation Program Components

Civicom certifies that as part of its robocall mitigation efforts it is taking these specific reasonable steps to avoid originating illegal robocall traffic:

5.1. Customer Vetting Procedures

Customers using the conferencing platform are either internal teams or pre-approved clients onboarded through Civicom's standard business processes.

5.2. Monitoring and Ongoing Review

The conferencing platform includes internal mechanisms that monitor for abnormal outbound call behavior and can send email alerts on suspicious patterns.

Currently, Civicom is evaluating options for a more comprehensive, network-wide SIP monitoring and alerting system. The goal is to strengthen robocall detection across all telephony components and ensure faster response to suspicious activity. Integration of such tools is under active consideration as part of our ongoing mitigation improvements.

5.3. Remediation and Enforcement

Civicom investigates and remediates any incident of suspected fraud or unauthorized calling activity involving its telephony platforms.

In the event of an incident, such as leaked conference credentials or compromised PBX extensions, the company initiates the following remediation steps:

- Immediate disabling of the affected access or feature (e.g., outbound dial-out)
- Resetting PINs/passwords and hardening access
- Notifying impacted users or customers
- Internal verification to determine if the activity was authorized or malicious

While no incidents have required regulatory reporting to date, Civicom remains prepared to report verified abuse to law enforcement or the FCC in accordance with applicable requirements. Affected accounts may be restricted, suspended, or permanently terminated based on the severity of the violation.

5.4. Acceptable Use Policy (AUP)

Civicom publishes and maintains an Acceptable Use Policy (AUP), available here: [Terms of Service](#). The AUP permits Civicom to terminate service to any Customer for numerous violations, including but not limited to unlawful Robocalls.

5.5. Prohibited Practices

Civicom prohibits the following practices on its conferencing and PBX platforms:

- Unauthorized use of outbound calling features (e.g., dial-out via leaked or shared credentials)
- Re-origination of PSTN traffic or any use of the platform for illegal call routing
- Use of spoofed or manipulated caller IDs to mislead recipients
- Accessing or registering to the PBX without permission (e.g., via guessed extensions)
- Use of services for unlawful, fraudulent, or malicious purposes

Any attempt to bypass call routing restrictions, falsify call identity, or otherwise misuse the system may result in service termination and escalation as required by law or FCC regulation.

5.6. Traceback Cooperation

Civicom certifies that it will respond to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. As of this filing date, Civicom has not received any such traceback requests.

Civicom certifies that it will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

5.7. Employee Training

Civicom maintains a structured training program tailored to the operational realities of its telephony systems and the distinct teams that manage them.

- **Annual robocall mitigation training** will be conducted for compliance staff, network operations, and customer support. This covers the legal landscape, robocall patterns, and mitigation responsibilities.
- **Specialized training** will be provided for those handling traceback requests, reviewing call records, and enforcing usage controls. This includes how to respond to ITG or FCC inquiries, validate traffic sources, and document incidents.

Apart from this, Civicom consistently provides Information Security (InfoSec) training for all employees. This training covers data protection frameworks, secure system usage, incident reporting procedures, and compliance with applicable security policies and regulatory requirements. Refresher courses are conducted regularly to ensure awareness remains current and aligned with evolving threats and best practices.

5.8. Complaint Handling Process

- Dedicated email and phone for robocall complaints
- Complaints logged, investigated within 10 business days
- Corrective actions documented and reviewed by compliance officer

5.9. Updates & Plan Maintenance

Civicom certifies that this Robocall Mitigation Plan will evolve to respond to the constantly changing practices and techniques that are used to detect and prevent illegal robocalling. Civicom will continue to monitor industry best practices and improve its internal processes to ensure that this Robocall Mitigation Plan is current. In the event of any material change to this Robocall Mitigation Plan, Civicom will submit an updated Robocall Mitigation Plan to the FCC's Robocall Mitigation Database.

6. Third-Party Vendor Controls

6.1. Due diligence conducted on upstream and downstream providers

6.2. Vendor audits performed annually

7. Compliance Officer Certification

Signed by:

Ma. Concepcion Pascua

Ma. Concepcion Pascua

InfoSec and Compliance Officer

02/25/2026

Audit trail

Details

FILE NAME	Copy of Robocall Mitigation Plan Template - 2/25/26, 3:49 PM
STATUS	Signed
STATUS TIMESTAMP	2026/02/26 14:27:26 UTC

Activity

SENT	lyziel.uy@civi.com sent a signature request to: Ma. Concepcion Pascua (macci.pascua@civi.com)	2026/02/25 20:50:12 UTC
SIGNED	Signed by Ma. Concepcion Pascua (macci.pascua@civi.com)	2026/02/26 14:27:26 UTC
COMPLETED	This document has been signed by all signers and is complete	2026/02/26 14:27:26 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.