

STEWARD IT LLC

Robocall Mitigation Program Description

FCC Robocall Mitigation Database Filing

Effective date: September 14, 2026

Version: 1.0

DBA: Steward IT

Entity type: Single-member limited liability company; non-facilities-based interconnected VoIP reseller

Underlying wholesale carrier: VoIP.ms

OCN: None (reseller; not a numbering administrator / carrier of record)

Principals, affiliates, subsidiaries, and parent companies: None

Robocall mitigation contact: Company Owner / Compliance

1. Purpose and Scope

This document describes the robocall mitigation program of Steward IT LLC (“Company”). The Company resells interconnected Voice over Internet Protocol (VoIP) service to end-user customers using the network of its wholesale provider, VoIP.ms. The Company does not own or operate public switched telephone network (PSTN) switches, session border controllers, or the SIP signaling infrastructure used to originate calls onto the PSTN.

This program is maintained to comply with 47 CFR § 64.6305, including the duty to take reasonable steps to avoid originating illegal robocall traffic, to know the Company’s customers, and to respond fully within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the registered industry traceback consortium.

2. Role in the Call Path and STIR/SHAKEN Status

The Company is a voice service provider without a STIR/SHAKEN implementation obligation. It serves end-user customers only. It is not a gateway provider and is not a non-gateway intermediate provider.

The Company has not implemented the STIR/SHAKEN authentication framework on any portion of a network of its own because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. See 47 CFR § 64.6305(d)(2)(i); Call Authentication Trust Anchor, First Report and Order, 35 FCC Rcd 3241, 3260 para. 40 (2020). The Company does not hold an STI-GA Service Provider Code (SPC) token and cannot digitally sign calls. Outbound calls placed by the Company’s end users are originated and authenticated by VoIP.ms, which controls the relevant SIP infrastructure and implements STIR/SHAKEN on that network. The Company does not accept or hand off wholesale voice traffic from other providers.

3. Know-Your-Customer (KYC) Procedures

The Company does not offer self-service online signup that allows anonymous or unverified origination of PSTN calls. Every voice customer is onboarded in person before service is activated.

Before activating service, the Company collects and retains:

- Legal name of the individual customer or of the customer’s business entity.
- Physical service / billing address. The Company does not accept a P.O. box as the sole customer address.
- Government-issued photo identification reviewed in person at onboarding.
- Working telephone number and email address for the account owner.

- Intended use of the service (for example, small-business or personal voice service).
- A unique internal customer number assigned by the Company and bound to each DID (telephone number) issued to that customer.

The in-person meeting is used to confirm that the person requesting service is who they claim to be, that the stated address is consistent with the identification presented, and that the requested use is ordinary voice communications rather than high-volume, short-duration, or unsolicited telemarketing traffic. The Company does not knowingly accept customers whose primary purpose is robocalling, lead generation by autodialer, neighbor spoofing, or traffic pumping.

Each DID remains associated in the Company's records with that customer number for the life of the assignment. If a number is reassigned, the prior association is closed and a new customer-number association is recorded. The Company can identify, from a calling number or account identifier, the responsible customer and the address collected at onboarding.

4. Account Controls and Prohibited Uses

Customers are prohibited from using the service to:

- Originate illegal robocalls or display a calling number the customer is not authorized to use.
- Display a Caller ID number the customer is not authorized to use.
- Originate traffic on behalf of an undisclosed third party or resell the Company's service without prior written approval.
- Engage in short-duration, high-volume outbound campaigns inconsistent with the use described at onboarding.

Outbound Caller ID number is limited to telephone numbers the Company assigned to the customer. Customers may not set an unassigned calling number. Customers may edit the Caller ID name (CNAM) shown with their assigned number.

5. Traffic Monitoring and Mitigation Steps

The Company's primary controls are in-person KYC and a small, known customer base. The Company does not operate a third-party call-analytics platform and does not review the destination numbers of ordinary customer calls. As part of normal billing, the Company reviews outbound minute usage. A sudden, unexplained spike in billed minutes or a complaint or traceback tied to a customer account is treated as a reason to investigate that account.

Network-level STIR/SHAKEN, call blocking, and related analytics, if any, are performed by the underlying carrier, VoIP.ms. The Company does not independently authenticate calls.

If illegal or apparently illegal robocall traffic is identified or reasonably suspected, the Company will:

- Immediately suspend outbound calling on the affected account and associated DIDs.
- Investigate the account against onboarding records and call detail.
- Require a satisfactory explanation and, if appropriate, terminate the account.
- Preserve relevant records and cooperate with traceback, the Commission, and law enforcement.

6. Traceback and Law-Enforcement Response

The Company commits to respond fully, and within 24 hours of receipt, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate in investigating and stopping any illegal robocallers that use its service. See 47 CFR § 64.6305(a).

Traceback and robocall inquiries should be sent to the robocall mitigation contact identified in the Company's Robocall Mitigation Database filing. The Company will identify the responsible customer from the calling number or customer number, provide the customer identifying information it has collected, state whether the traffic was authorized by that customer, and take the mitigation steps in Section 5. The Company will not delay a traceback response in order to notify the customer first when doing so would impede the investigation.

7. Record Retention

The Company retains its own KYC records for at least two years, and longer if a traceback, complaint, or investigation is pending. Those records include the customer's name, address, the date of the in-person onboarding meeting, confirmation that identification was reviewed, the internal customer number, and the DID(s) assigned to that customer number.

Call detail records are generated and stored by VoIP.ms. The Company accesses those records in the wholesale portal as needed for billing and traceback. The Company does not operate a separate call-recording archive. If a traceback or investigation is pending, the Company will export and retain the relevant CDRs from the wholesale portal.

8. Point of Contact

Robocall mitigation, traceback, and related regulatory inquiries are handled by the Company Owner (Compliance). Current name, telephone number, email address, and mailing address are those listed in the Company's active Robocall Mitigation Database filing and FCC CORES record for Steward IT LLC.

9. Review and Updates

This program will be reviewed at least annually and whenever the Company's service model, upstream carrier, or FCC robocall rules materially change. The Company will update its Robocall Mitigation Database filing when required, including annual recertification.

10. Certification

The undersigned officer certifies that this document is the Company's robocall mitigation program; that the Company takes reasonable steps to avoid originating illegal robocall traffic; and that the Company will respond fully within 24 hours to traceback requests as described above.

Signature: _____

Name: _____

Title: Owner / Managing Member

Date: September 14, 2026