

Robocall Mitigation Program Description

Prepared for submission to the Federal Communications Commission Robocall Mitigation Database

Effective date July 22, 2026

Version 1.0

Program scope

United States-based healthcare customers; individually requested return calls; written, revocable healthcare-reminder authorization; customer due diligence; caller-identity controls; traffic monitoring; enforcement; and 24-hour traceback response.

This description applies to the Filer identified by the associated FCC Robocall Mitigation Database submission.

1. Purpose and scope

The Filer maintains this Robocall Mitigation Program to prevent its network and services from being used to originate illegal robocalls, unlawful spoofing, fraud, or other abusive calling. The program applies to every customer, telephone number, endpoint, and call originated through the Filer's network.

The Filer takes reasonable and effective steps to avoid originating illegal robocall traffic, responds fully within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the registered Industry Traceback Group, and cooperates with those entities in investigating and stopping illegal callers.

At the effective date of this description, the Filer is completing deployment of a new voice network. It will not activate production origination until the applicable customer-verification, access-control, caller-identity, monitoring, recordkeeping, and enforcement controls described in this program are operational. Every production call originated by the Filer will be subject to this program.

2. Business model and risk profile

The Filer provides voice services exclusively to verified United States-based healthcare facilities. Restricting service to a defined domestic industry materially improves the Filer's ability to validate customer identity, intended use, telephone-number authority, and expected calling behavior. Healthcare status is an input to due diligence and is not treated as proof that any particular call is lawful.

Expected traffic consists of:

- ordinary person-to-person healthcare and business communications;
- return calls individually requested by the person receiving the call; and
- healthcare reminders supported by written, revocable authorization from the called person or a legally authorized representative.

The Filer prohibits telemarketing, political calling, lead generation, mass marketing, and use of its service by third-party debt collectors. A healthcare facility may contact its own patient regarding a balance owed to that facility as part of the existing provider-patient relationship, subject to all applicable consent, identification, calling-method, and opt-out requirements. The Filer does not provide service to debt-collection businesses or permit collection activity on behalf of unrelated third parties. Unauthorized robocalling is prohibited.

3. Know Your Customer and customer acceptance

No customer may originate traffic until the Filer completes identity, authority, business-purpose, and risk review. The Filer obtains and evaluates information sufficient to know the customer, including:

- legal business identity, organization type, active status, physical United States address, and reliable contact information;
- the identity and authority of the individual opening or controlling the account;
- evidence that the applicant is a healthcare facility, using appropriate licensing, provider, business, or other authoritative records;
- a business website, email domain, telephone information, and payment relationship reasonably consistent with the applicant's identity;
- requested telephone numbers and evidence that the applicant is entitled to use them;
- intended calling purposes, anticipated volume and calling patterns, destinations, and requested service features; and
- inconsistencies, adverse information, fraud indicators, or other facts requiring enhanced review.

The Filer rejects or escalates applications containing incomplete, inconsistent, unverifiable, or suspicious information. Successful payment alone is not sufficient for activation. The Filer may require additional documentation, direct confirmation with the facility, or management review.

Material changes to identity, control, service purpose, telephone numbers, traffic characteristics, payment information, or technical access trigger re-verification. Active accounts are reviewed periodically and when risk indicators, complaints, traceback activity, or anomalous traffic warrant review.

4. Contractual and acceptable-use controls

Each customer must agree to Terms and Conditions and an Acceptable Use Policy that prohibit unauthorized robocalls and unlawful caller-ID practices. The customer is responsible for the legality, content, consent, authorization, and caller identity associated with its calls.

Prohibited conduct includes:

- unauthorized artificial-voice, prerecorded-message, autodialed, or mass calling;
- transmitting a caller identity the customer is not entitled to use;
- caller-ID spoofing intended to defraud, cause harm, or wrongfully obtain value;
- fraud, impersonation, phishing, harassment, or deceptive calling;
- use of purchased, scraped, or improperly obtained calling lists;
- undisclosed resale or subdelegation of service;
- evasion of rate limits, identity controls, blocking, traceback, or investigation; and
- calling that violates the Telephone Consumer Protection Act, FCC rules, Federal Trade Commission rules, or applicable state law.

The agreements authorize the Filer to investigate suspected abuse; request consent, authorization, or business-purpose evidence; reject calls; restrict rates, destinations, telephone numbers, or features; suspend service immediately when necessary; and terminate service for violations.

5. Controls for requested return calls and reminders

5.1 Individually requested return calls

Each use of the return-call feature must result from a specific request by the person who will receive that call. A request for one return call is not treated as blanket consent for unrelated, recurring, or marketing calls.

The Filer's call-return modules log request and call history sufficient to correlate the outbound call to its triggering request. The history includes the originating caller information available to the module, the requested callback number, the facility, relevant timestamps, and the resulting call. This permits the Filer to investigate a complaint even when the caller requested a callback to a number different from the number used to make the request.

When a complaint or abuse pattern involves an alternate callback number, the Filer can use the request history to take proportionate action. Actions may include blocking future callback requests to the alternate number, restricting the source or customer workflow, preserving relevant records, and escalating or suspending the customer when appropriate. Repeated calls inconsistent with an individually requested return call may be limited, suspended, or investigated.

5.2 Healthcare reminders

Healthcare reminders are permitted only when supported by written, revocable authorization obtained by the healthcare facility from the called person or a legally authorized representative. The authorization must reasonably identify the telephone number, healthcare facility, and scope or purpose of the reminders. As a condition of service, each healthcare customer certifies to the Filer that it obtains and maintains the required authorization and follows a process for honoring revocation.

The healthcare facility maintains the underlying patient authorization records. The Filer does not routinely collect or retain patient medical records or patient consent documents as part of this program. A customer must respond promptly to a compliance inquiry, confirm whether valid authorization was maintained for the call at issue, honor any revocation, and take corrective action. Records required by lawful process are handled through the appropriate secure and legal procedure.

Customers must provide a practical way to revoke authorization and must apply revocation promptly to the relevant calling workflow. Reminder content must remain within the authorized healthcare purpose. Marketing or advertising is not converted into a healthcare communication merely because it accompanies a healthcare-related message. Artificial or prerecorded messages must satisfy all applicable identification, contact, consent, and opt-out requirements.

6. Telephone-number and caller-identity controls

Customers may present only telephone numbers assigned to them by the Filer or independently verified as numbers they are entitled to use. The Filer binds approved caller identity to the customer account and authorized route. Arbitrary or unauthorized customer-supplied caller ID is rejected or corrected.

Forwarded calls are treated separately from customer-originated calls. For an inbound call that is forwarded to an external destination, the Filer preserves the original calling-party identity and available inbound authentication information. The forwarding customer may not replace that identity with an arbitrary calling number. The Filer records the forwarding customer, original caller, original called number, forwarding destination, presented caller identity, and both call legs so the call remains attributable and traceable.

When STIR/SHAKEN diversion authentication is operational and applicable, the Filer will preserve valid original authentication and apply standards-compliant diversion authentication for the changed destination. It will not represent that the original caller's telephone number belongs to the forwarding customer or the Filer, and it will not create an unsupported attestation for that number.

The Filer's production controls require it to:

- validate authority to use a telephone number before enabling it;
- suspend or remove numbers when authority expires, is disputed, or cannot be reverified;
- prevent origination using invalid, unallocated, or unauthorized numbers;
- apply applicable do-not-originate blocking requirements;
- preserve the originating customer and asserted identity in call records; and
- investigate material changes in calling number, destination mix, or volume.

The Filer is implementing STIR/SHAKEN authentication for calls it originates as the required registration, numbering, token, certificate, and interoperability prerequisites become available. Its implementation status and any applicable exemption are reported separately and accurately in its Robocall Mitigation Database filing. Until signing is operational, the Filer relies on its KYC, telephone-number binding, access controls, traffic monitoring, and enforcement program to protect caller-identity integrity.

7. Network access and routing controls

The Filer accepts origination only from provisioned customers and specifically authorized endpoints. Anonymous public origination is not permitted. Depending on the service, controls include approved source networks, strong credentials or certificates, encrypted signaling where supported, customer-specific trunk definitions, and source-address validation.

The Filer establishes customer-appropriate controls for calls per second, concurrent calls, source addresses, signaling transports, calling-number ranges, destination classes, forwarding, and other routing features. Changes made through administrative or customer-facing systems are authenticated, authorized, validated, and recorded in an audit trail attributable to the actor. The Filer can disable an account, endpoint, number, destination, or feature without a disruptive router restart.

Routing and accounting records identify the customer, source endpoint, calling and called numbers, routing attempts, selected carrier, response, and responsible SIP-router instance. SIP observability and call-detail records support rapid investigation and traceback.

8. Traffic monitoring and detection

The Filer monitors originated traffic for behavior inconsistent with the verified customer profile or lawful healthcare use. Risk indicators include:

- unexpected increases in call attempts, calls per second, concurrency, or duration;
- unusual time-of-day behavior, destination concentration, geographic anomalies, or rapid number rotation;
- unusually short calls, repeated unanswered calls, retry bursts, or abnormal answer and failure ratios;
- new, invalid, unallocated, or unverified calling numbers;
- patterns inconsistent with individually requested return calls or authorized reminders;
- customer, carrier, called-party, law-enforcement, or traceback complaints;
- STIR/SHAKEN identity or attestation anomalies after signing becomes active; and
- attempts to bypass controls or resume previously restricted behavior.

Monitoring information is obtained from call-detail records, SIP signaling and routing telemetry, customer and endpoint configuration, carrier responses, system alerts, complaints, and traceback requests. Alerts are prioritized according to severity, scale, customer risk, and potential harm. High-risk activity is investigated promptly and may be suspended before the investigation is complete.

9. Investigation and enforcement

The Filer uses a risk-based response. It may:

1. reject a call or block a calling number or destination;
2. reduce rate or concurrency limits;
3. disable automation, forwarding, or other features;
4. require the customer to confirm authorization status or produce non-patient business-purpose and compliance evidence;
5. suspend an endpoint or the entire account;
6. terminate service; and
7. preserve records and cooperate with carriers, the Industry Traceback Group, the FCC, and law enforcement.

When continued traffic may cause harm or frustrate an investigation, the Filer may suspend service first and investigate immediately afterward. Restoration requires a documented determination that the risk has been resolved and that appropriate corrective controls are in place. Intentional, repeated, or material violations are grounds for termination.

10. Complaints and traceback response

The Filer maintains the abuse and traceback contact identified in its regulatory registration and monitors that contact so requests can be acted upon without delay. Requests are logged, assigned, investigated, and preserved.

For an authorized traceback, the Filer uses call-detail, SIP-routing, carrier, customer, endpoint, telephone-number, and administrative audit records to identify the source and the next or previous provider. The Filer commits to provide a full response within 24 hours and to take prompt protective action when the traffic is illegal or materially suspicious.

The response record identifies the request, receipt time, call identifiers, findings, records supplied, customer action, network action, responder, and completion time. Backup coverage and periodic exercises reduce dependence on any one employee.

11. Interconnected-provider due diligence

The Filer performs risk-appropriate due diligence before accepting traffic from or sending traffic to another provider. This includes verifying provider identity and contacts, intended service relationship, applicable Robocall Mitigation Database status, and material adverse indicators. Written relationships require cooperation with traceback, caller-ID integrity, and lawful traffic requirements.

The Filer does not knowingly accept directly connected upstream traffic from a provider that lacks a required Robocall Mitigation Database filing. It takes prompt action in response to FCC notices, traceback findings, or other credible evidence that a connected provider is a source of illegal traffic.

12. Records, training, and governance

The Filer retains records sufficient to demonstrate operation of the program, including customer-verification reviews, customer agreements and certifications, telephone-number authorization, risk profiles, configured limits, callback-module history, call and routing records, alerts, complaints, investigations, enforcement actions, and traceback responses. Healthcare customers retain the underlying patient authorization records; the Filer does not routinely collect or retain patient medical records or patient consent documents as part of this program.

Program and enforcement records are retained for at least five years after creation or account termination, as applicable, unless a longer period is required by law, contract, litigation hold, or an active investigation. Records are protected against unauthorized access and handled consistently with applicable privacy and security obligations.

Personnel responsible for onboarding, support, network operations, abuse response, and compliance receive role-appropriate training. The program is reviewed at least annually and after a material service change, significant enforcement event, regulatory change, or identified control failure. The Filer corrects documented deficiencies and updates its Robocall Mitigation Database certification when its implementation status or program materially changes.

13. Management commitment

Management has adopted this program as a condition of providing voice service. Compliance is not delegated solely to customers or carriers. The Filer maintains responsibility for operating its own preventive controls, evaluating risk, responding to traceback, and acting to stop unlawful traffic that originates through its network.

Regulatory references

- 47 C.F.R. Section 64.6305, Robocall mitigation and certification requirements.
 - 47 C.F.R. Section 64.1200, calling restrictions, identification, opt-out, customer due diligence, and do-not-originate requirements.
 - 47 C.F.R. Section 64.6304, STIR/SHAKEN exemptions.
 - FCC, Robocall Mitigation Database Filing Instructions and Frequently Asked Questions, January 2026.
-

Document control

Version 1.0 | Effective July 22, 2026 | Review at least annually and after material changes to the service, program, or governing requirements.