

Robocall Mitigation Program

Forward Runtime Inc. · Public filing version · Effective August 21, 2026

LEGAL ENTITY	PRINCIPAL OFFICE
FORWARD RUNTIME INC California corporation	As listed in the company's CORES and RMD records
RESPONSIBLE OFFICER	PROVIDER MODEL
Chief Executive Officer Name and contact information as listed in the RMD filing	Non-facilities-based voice service provider Serving business end users through upstream carrier services

Purpose and commitment

Forward Runtime Inc. ("Forward Runtime") maintains this program to prevent its network, platform, and services from being used to originate, transmit, or facilitate illegal robocalls or unlawfully spoofed calls. The company applies affirmative, effective controls proportionate to its current services and risk profile and will revise those controls as its products and traffic change.

Forward Runtime is initially focused on inbound, business-to-business voice automation. Any outbound calling is limited to legitimate operational communications requested or reasonably expected by the receiving business, such as a laboratory contacting a medical office to clarify an order. Forward Runtime does not permit cold prospecting, lead-generation robocalling, or high-volume unsolicited calling.

This document describes operational safeguards. It does not replace any separate obligation imposed by the Communications Act, FCC rules, the Telephone Consumer Protection Act, state law, contractual requirements, or industry standards.

1. Services and call-chain role

Forward Runtime provides software-enabled voice functionality to business customers and uses Bandwidth Inc. as its upstream communications provider. Forward Runtime does not operate its own physical telecommunications network. For RMD purposes, it files as a voice service provider serving end users and does not represent itself as a gateway provider or non-gateway intermediate provider.

Typical permitted use cases

- Inbound calls to a business that are answered by an automated assistant configured for that business.
- Customer-care and operational communications between businesses with an existing relationship.
- A requested follow-up text containing a summary or other information discussed during a call.
- Limited outbound calls needed to complete an existing transaction or clarify submitted information.

2. STIR/SHAKEN and caller-ID authentication

Forward Runtime recognizes that caller-ID authentication is an important component of preventing illegal spoofing. The company is coordinating with its upstream provider to confirm and implement the authentication method applicable to its provider role, including hosted signing where appropriate. Forward Runtime will not knowingly originate production outbound traffic in a manner inconsistent with applicable STIR/SHAKEN requirements.

Before enabling material outbound calling, Forward Runtime will complete the technical and administrative prerequisites required for the selected authentication model, maintain accurate calling-party information, and ensure that authorized telephone numbers are used. It will update its RMD filing within the required period if its implementation status or call-chain role changes.

3. Know-your-customer program

Forward Runtime identifies and evaluates each business customer before enabling voice service. Review depth is risk-based and may include the following:

- Legal business name, physical address, website, jurisdiction, and formation or registration records.
- Identity, role, business email, and authority of the representative opening the account.
- Intended voice and messaging use cases, target recipients, anticipated volume, and expected traffic patterns.
- Evidence of the customer's relationship with intended recipients and its consent or permission process.
- Review of inconsistencies, unverifiable claims, suspicious domains, unusual payment details, or elevated-risk use cases.
- Additional documents or enhanced review when information is incomplete, inconsistent, or higher risk.

Forward Runtime will not activate an applicant whose identity, authority, business purpose, or intended use cannot be reasonably verified. It may delay activation, restrict features or volume, require additional evidence, or reject the applicant.

4. Customer obligations and acceptable use

Customers must use the service only for lawful, authorized purposes. Contractual terms and onboarding materials prohibit customers and their users from:

- Originating illegal, fraudulent, deceptive, threatening, harassing, or abusive calls.
- Spoofing or manipulating caller identification, impersonating another party, or using numbers without authorization.
- Conducting unsolicited mass calling, cold prospecting, lead generation, or campaigns lacking required consent.
- Circumventing traffic limits, identity checks, complaint controls, number blocking, or provider safeguards.
- Using automated agents to extract sensitive data, commit fraud, or interfere with another automated or human system.
- Violating calling-hour restrictions, do-not-call requirements, revocation requests, or other applicable law.

Customers are responsible for maintaining records sufficient to demonstrate that their calls are wanted and lawful. Forward Runtime may request those records during onboarding or investigation.

5. Consent and wanted-call controls

Forward Runtime's initial services are designed primarily for inbound communications initiated by the caller. When an end user asks during a call to receive a text or other follow-up, the system records the request and limits the follow-up to the requested information. Written opt-in interfaces, when used, clearly identify the sender, describe the message purpose, present required disclosures, and record the affirmative action used to consent.

For outbound voice communications, the customer must establish a legitimate business purpose and maintain any consent, contractual permission, or other legal basis required for the call. Revocation, opt-out, and do-not-call requests must be honored promptly and propagated to the applicable suppression controls.

6. Traffic monitoring and analytics

Forward Runtime uses available platform, carrier, and application data to identify conduct inconsistent with a customer's approved use case. Signals may include abrupt volume changes, repeated short-duration calls, high failure or rejection rates, repeated calling to unrelated destinations, caller-ID anomalies, recipient complaints, traceback requests, and attempts to evade controls.

Forward Runtime currently relies on its own application controls and information made available by Bandwidth. It does not currently use a separate third-party robocall analytics vendor. If that changes, this plan and the RMD filing will be updated as required.

7. Detection, investigation, and mitigation

Forward Runtime reviews credible indications of unlawful or abusive calling promptly and applies measures proportionate to the evidence and urgency. It may act before completing an investigation when necessary to prevent ongoing harm.

STAGE	ACTION
Triage	Preserve relevant account, call, number, complaint, and configuration information; assess immediacy and scope.
Investigate	Compare activity with the approved use case, review identity and consent records, and request an explanation or supporting evidence.
Contain	Rate-limit, block destinations or numbers, disable outbound functionality, suspend the account, or reject calls before answer where appropriate.
Remediate	Require corrective controls, retraining, configuration changes, reverification, or written assurance before restoring service.
Terminate and escalate	Terminate service for confirmed, repeated, or serious violations and notify Bandwidth, traceback authorities, regulators, or law enforcement when appropriate.

Inbound abuse

Forward Runtime maintains application-level controls to reject known blocked callers before answer and to terminate abusive interactions. Because number reputation alone cannot reliably identify every newly assigned or rotated number, Forward Runtime combines number history with observed behavior and customer-specific blocking decisions rather than treating a previously unseen number as unlawful by default.

8. Traceback and government cooperation

Forward Runtime commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the registered industry traceback consortium. The responsible contact listed in the RMD filing is monitored for these requests. Forward Runtime will preserve relevant records, identify the customer and upstream path, provide responsive information permitted by law, and take prompt action to stop confirmed illegal traffic.

9. Upstream-provider diligence

Forward Runtime obtains communications services from Bandwidth Inc. and maintains operational and escalation channels with that provider. It reviews applicable compliance guidance and cooperates with Bandwidth and other providers on customer validation, call authentication, traceback, complaint response, suspicious-traffic investigation, and traffic mitigation. Before adding another upstream provider, Forward Runtime will evaluate the provider's identity, regulatory standing, RMD status where applicable, and ability to support lawful caller authentication and traceback.

10. Records, training, and governance

- Maintain appropriate customer identity, onboarding, authorization, consent, configuration, complaint, and investigation records.
- Limit access to sensitive customer and call data according to job responsibility.
- Train personnel responsible for onboarding, operations, support, and compliance on escalation and preservation procedures.
- Review material complaints, traceback activity, traffic changes, and provider notices to identify control improvements.
- Escalate significant or repeated concerns to the responsible officer.

11. Review and updates

The responsible officer reviews this program at least annually and when Forward Runtime introduces a material new calling use case, changes upstream providers, changes its STIR/SHAKEN implementation, experiences a significant incident, or identifies a material control weakness. Forward Runtime will update its RMD filing within the period required by FCC rules when filed information changes and will complete required annual recertification.

Certification note	This public program description is intended to accompany Forward Runtime's RMD filing. The officer signing the portal declaration should confirm that the provider-role and STIR/SHAKEN selections in the portal accurately reflect the company's status on the execution date.
-------------------------------	---

Approved by

Chief Executive Officer · Forward Runtime Inc.
Effective date: August 21, 2026