

ROBOCALL MITIGATION PROGRAM

Internal compliance document supporting FCC Robocall Mitigation Database submissions
25 State St Apt 2F, Ossining, NY 10562
Primary contact: Joel Brito • info@extrv.biz
Version 1.0 • March 10, 2026

This program describes the reasonable steps EXTRV LLC takes to prevent the origination of illegal robocalls, to validate customer use of telephone numbers, to investigate suspicious traffic, and to cooperate with upstream providers and traceback requests. EXTRV LLC also offers SMS-enabled workflows; however, this document is focused on voice traffic and related robocall-mitigation controls.

1. Executive Summary

EXTRV LLC operates an AI-powered business communications platform used by legitimate business customers for customer-service, appointment, reminder, notification, support, and other lawful customer-engagement use cases. Calls that are originated from the platform are subject to account screening, telephone-number validation, traffic monitoring, complaint handling, and immediate suspension procedures where suspicious activity is identified.

Legal name	EXTRV LLC
Business model	AI-powered communication platform for small businesses; voice plus messaging workflows
RMD focus	Voice traffic originated for lawful business communications; SMS/A2P registration handled separately as applicable
Call-chain role	Originating voice service provider serving end users/business customers
STIR/SHAKEN status	Calls are originated through compliant upstream voice service providers that implement authentication where applicable
Primary compliance owner	Joel Brito (joel@extrv.biz)

2. Purpose and Scope

This program is maintained to support EXTRV LLC's FCC Robocall Mitigation Database filing and related carrier-compliance reviews. It describes the specific, reasonable, and affirmative steps the company takes to reduce the risk that illegal robocall traffic will originate from its platform.

This program applies to voice traffic originated using EXTRV LLC's platform, customer onboarding and renewal activity, number-use validation, complaint handling, traceback support, relationships with upstream voice providers, and internal response procedures for suspicious activity. While EXTRV LLC may also support SMS-enabled workflows, the present document is focused on voice controls that relate directly to robocall mitigation obligations.

- Applies to new and renewing customers using voice functionality.
- Applies to calls placed through upstream carriers or SIP partners selected by EXTRV LLC.

- Applies to any outbound voice campaign, transactional communication, support callback, or AI-assisted calling workflow launched from the platform.
- Applies to complaints, carrier notices, traceback requests, blocking events, and internal audits.

3. Company Role in the Call Chain and STIR/SHAKEN Status

EXTRV LLC functions as an originating voice service provider for calls initiated by its business customers through the platform. In practical terms, EXTRV LLC provides the application layer, customer workflow layer, AI interaction layer, and traffic-governance layer, while upstream voice service providers provide the network interconnection, signaling, and delivery path into downstream networks.

EXTRV LLC does not directly operate the underlying PSTN gateway or signing infrastructure required to perform STIR/SHAKEN caller-ID authentication independently across the network path. Where caller-ID authentication is available, EXTRV LLC relies on compliant upstream voice service providers to implement authentication within their controlled network environment. Accordingly, EXTRV LLC maintains a robocall mitigation program focused on customer verification, number authorization, traffic oversight, traceback cooperation, and rapid account suspension when suspicious activity is detected.

- Role: originating voice service provider serving end users/business customers.
- Model: platform-originated traffic sent through upstream carriers and SIP interconnection partners.
- Authentication posture: upstream-provider implementation where technically and contractually available.
- Mitigation posture: proactive screening, monitoring, intervention, and records retention.

4. Services Covered by This Program

EXTRV LLC is designed for lawful business-to-customer communications. Authorized use cases include appointment reminders, support callbacks, service notifications, customer-service interactions, account follow-up, complaint resolution, reservation or scheduling coordination, lead qualification where legally permitted, and other consent-based or otherwise lawful business communications.

The platform is not intended for unlawful telemarketing, deceptive caller-ID use, mass unsolicited calling, prank or harassment traffic, premium-rate exploitation, or any use designed to evade consumer choice, carrier rules, or applicable law.

- Permitted: customer support, reminders, notifications, and operational business communications.
- Restricted or prohibited: fraudulent, deceptive, abusive, or unlawful calling activity; unlawful prerecorded campaigns; spoofing; and any traffic that misrepresents the caller or purpose of the call.
- Separate treatment of messaging: SMS workflows are governed under separate A2P and sender-registration requirements where applicable and are not a substitute for voice compliance obligations.

5. New and Renewing Customer Controls

EXTRV LLC uses affirmative and effective onboarding controls designed to prevent new and renewing customers from originating illegal calls. These controls are risk-based and may be enhanced for customers that intend to use higher volumes, automated workflows, artificial voices, or sensitive use cases.

5.1 Customer Identity and Business Verification

Before production voice functionality is enabled, EXTRV LLC collects sufficient information to identify the customer, understand the business use case, and establish the relationship between the customer and the telephone numbers or campaigns the customer intends to use.

- Legal business name and operating identity.
- Primary business contact and contact information.
- Business website or other corroborating business presence where available.
- Description of intended calling use cases and expected traffic profile.
- Review of whether the customer is acting on its own behalf or on behalf of another business.

5.2 Renewal and Material-Change Review

Customer reviews are repeated at renewal or whenever there is a material change in the customer's business, ownership, number inventory, traffic pattern, or use case. EXTRV LLC may require refreshed documentation before permitting expanded traffic or newly automated workflows.

- Recheck contact details and account ownership.
- Reconfirm use cases and campaign purpose.
- Review complaint history, blocking history, and prior enforcement actions on the account.
- Escalate higher-risk accounts for manual approval before additional traffic is enabled.

5.3 Contractual and Policy Controls

EXTRV LLC requires customers to agree to terms of service and acceptable-use restrictions that prohibit illegal robocalls, unauthorized prerecorded traffic, deceptive practices, spoofing, and use of numbers that the customer does not own or control. The company reserves the right to suspend or terminate service immediately where suspicious or unlawful activity is detected.

- Use restrictions are included in customer-facing agreements or onboarding materials.
- Customers may be required to certify that their traffic is lawful and consent-based where applicable.
- EXTRV LLC may refuse activation for customers that decline reasonable compliance checks.

6. Caller ID, Number Authorization, and CLI Governance

Accurate caller identification is a core control within EXTRV LLC's platform. The platform is designed to support authorized business identity use and to prevent customers from presenting misleading or unauthorized caller IDs.

- Customers may use only numbers that are assigned to them, provided through approved inventory, or otherwise demonstrably authorized for the intended campaign or workflow.
- Numbers that appear invalid, unassigned, high-risk, or inconsistent with the account profile may be blocked or subjected to manual review.
- Rotating, random, misleading, or impersonating caller IDs are prohibited.
- Where branded calling or CNAM features are used, the business identity must match the customer's verified business use case.

6.1 Number-Use Review

For new number onboarding, EXTRV LLC reviews the relationship between the customer and the presented caller ID. The company may request proof of assignment, purchase, or delegated authority before enabling the number for production use.

6.2 Caller-ID Enforcement

If a number is reported as unauthorized, repeatedly blocked, or associated with suspicious traffic, EXTRV LLC can immediately disable its use, remove it from customer campaigns, and require additional documentation before reactivation.

7. Traffic Monitoring, Analytics, and Operational Controls

EXTRV LLC monitors voice activity for indicators of illegal robocalling, fraudulent origination, or policy evasion. Monitoring is proportionate to account risk and may be performed through a combination of internal dashboards, system alerts, support review, and upstream provider notifications.

- Abnormal call spikes, burst dialing, or rapid campaign expansion inconsistent with the approved use case.
- Very short call attempts, repeated call failures, and other patterns that resemble dialer abuse or route testing associated with fraudulent activity.
- Repeated traffic to high-risk destinations or unusual geographies inconsistent with the customer profile.
- Large volumes of calls from newly activated accounts before trust is established.
- Patterns indicating repeated use of blocked or unauthorized caller IDs.
- Complaints from called parties, carriers, or analytics partners indicating spam-labeled behavior.

7.1 Risk Thresholds and Manual Escalation

When traffic exceeds predefined expectations or triggers suspicious patterns, EXTRV LLC escalates the account for review. Responses may include temporary rate limiting, call blocking, manual investigation, or full suspension pending customer clarification.

- Lower limits may be applied to new accounts or unseasoned numbers.
- Higher-risk campaigns may be placed in a monitored or approval-only state.
- Campaigns involving automated voices or large outbound volumes may require additional review before launch.

7.2 Upstream Signals and Carrier Feedback

EXTRV LLC considers carrier notices, blocking events, traceback alerts, spam-labeling indications, and other upstream feedback to be high-priority indicators of possible illegal traffic or policy non-compliance. Such signals trigger immediate operational review.

8. Know-Your-Upstream Provider Procedures

Because EXTRV LLC uses upstream voice service providers and SIP interconnection partners to originate traffic, the company maintains procedures designed to understand who its upstream providers are, what services they provide, what compliance obligations they impose, and how complaints or traceback requests are handled.

- Document the legal identity and contact information of upstream providers and wholesale partners.
- Review the provider's technical interconnection method, authentication model, and routing scope.
- Review whether the provider requires RMD, STIR/SHAKEN, KYC, or other compliance information before enabling routes.
- Prefer providers with clear abuse-handling processes and responsive operational support.
- Maintain records of route activation, blocking events, and provider communications related to suspicious activity.

8.1 Escalation with Upstream Providers

When EXTRV LLC receives a complaint, traceback request, or carrier abuse notice, the company coordinates promptly with the relevant upstream provider to review the specific call details, isolate the traffic source, and stop any suspicious or unlawful activity.

9. Complaint Handling, Traceback, and Cooperation

EXTRV LLC treats complaints and traceback requests as urgent compliance events. The company maintains procedures to identify the relevant account, number, traffic window, and technical call details quickly so that suspected illegal traffic can be isolated and, if appropriate, stopped without delay.

- Capture complaint source, date, time, called number, caller ID presented, and any supporting evidence available.
- Match the complaint to internal call records and account information where possible.
- Preserve relevant records while the matter is under review.
- Escalate suspected unlawful activity to compliance/operations personnel immediately.
- Cooperate with traceback consortium requests, carrier inquiries, and lawful regulatory inquiries within required or commercially reasonable timeframes.

-

9.1 Response Timeline

Where a traceback or upstream abuse inquiry is received, EXTRV LLC aims to acknowledge and begin review promptly and to provide a substantive response as quickly as practical, including coordination with upstream providers if the requested data is carrier-side. Accounts associated with serious complaints may be frozen before the investigation is complete.

9.2 Corrective Actions

Corrective actions may include number disablement, campaign disablement, account suspension, enhanced verification, traffic throttling, or permanent termination. Where an error is identified, operational controls are updated to reduce recurrence.

10. Account Suspension, Blocking, and Enforcement

EXTRV LLC reserves the right to suspend, limit, or terminate service immediately when there is evidence of illegal robocalling, caller-ID spoofing, unauthorized number use, fraudulent onboarding information, or any traffic pattern that presents unreasonable compliance risk.

- Temporary traffic suspension during investigation.
- Immediate disablement of specific caller IDs or campaigns.
- Reduced calling limits for accounts under review.
- Permanent account termination for confirmed abusive or unlawful use.
- Retention of evidence and records supporting the enforcement action.

11. Recordkeeping and Audit Trail

EXTRV LLC maintains records reasonably necessary to support compliance review, complaint investigation, and carrier-response obligations. Records may include onboarding information, number-authorization information, call-detail information, account changes, tickets, complaints, and communications with upstream providers.

Records are retained according to operational and legal requirements and are made available internally for audit, investigation, and remediation purposes. The precise retention period may vary depending on the record type and applicable obligations.

- Customer identity and onboarding records.
- Approved caller IDs and related authorization evidence.
- Call detail records and campaign metadata where available.
- Complaint logs, blocking notices, traceback requests, and investigation notes.
- Provider communications and carrier remediation actions.

12. Governance, Training, and Program Maintenance

Responsibility for this program sits with EXTRV LLC management and designated operations personnel. The program is reviewed periodically and updated whenever the company's service model, upstream carrier relationships, product features, or regulatory obligations change in a way that could affect robocall-mitigation controls.

Personnel responsible for customer onboarding, technical operations, or abuse handling are expected to understand the company's acceptable-use rules, escalation paths, and suspension authority. Training and process updates may be informal for a small organization but must be sufficient to ensure prompt and consistent handling of suspicious traffic.

- Review and update this document when services, providers, or risk controls materially change.
- Document significant policy or operational changes affecting robocall mitigation.
- Use lessons learned from complaints, blocking events, or provider feedback to improve controls.

13. Certification Support Statement

This robocall mitigation program is intended to provide a detailed description of the specific measures EXTRV LLC uses to avoid the origination of illegal robocalls, to prevent unlawful caller-ID use, to monitor account behavior, and to respond to complaints and traceback requests. The program is designed to be responsive to carrier onboarding reviews and FCC Robocall Mitigation Database filing requirements.

EXTRV LLC will continue to refine this program as traffic volume, product functionality, and regulatory requirements evolve. If the company later directly controls network infrastructure necessary for STIR/SHAKEN implementation or adopts additional third-party analytics or compliance vendors, this program will be updated accordingly.

14. Authorized Contact

Name	Joel Brito
Title	Authorized representative / compliance contact
Email	info@extrv.biz
Document date	March 10, 2026



Note: This document should be reviewed and refreshed whenever EXTRV LLC adds new traffic types, direct carrier arrangements, or material changes to its compliance program.