

Step 1: Proactive Monitoring and Detection

- Implement continuous detection of suspected robocalls using proactive management within the sky switch PBX for high activity volume, CNAM/SID analysis, STIR/SHAKEN signals, and real-time call analytics.
- Establish automated threat scoring and threshold-based alerts for anomalous activity.
- Maintain a centralized dashboard with key metrics: volume, regions, carriers, and action status.
- Schedule regular health checks of monitoring pipelines and data integrity.

Step 2: Customer Notification and Consent

- Notify customers of robocall remediation measures prior to or at the point of service activation.
- Provide clear, plain-language explanations of what mitigations may apply to their lines.
- Obtain explicit customer consent for specific remediation actions when required by policy or regulation.
- Offer channels for customers to opt out of non-critical mitigation where permissible.

Step 3: Mitigation Actions and Service Adjustments

- Apply least-disruptive mitigations first (e.g., call-filtering rules, rate-limiting, risk-based traffic scrubbing).
- Escalate to more stringent actions (e.g., temporary suspension or blocking of specific numbers) only after predefined risk criteria are met.
- Document each action with timestamps, rationale, and affected identifiers for auditability.
- Maintain a rollback plan and notification if a mitigation action impacts legitimate traffic.

Step 4: Terms and Conditions for Robocall Mitigation in the Contract

- Include a Robocall Mitigation clause describing permitted actions, data use, and customer responsibilities.
- Define service-level expectations for detection, notification, and remediation timelines.
- State that mitigations will be applied in a least-disruptive manner, with escalation procedures.
- Ensure compliance with applicable laws, privacy protections, and data retention policies.

Step 5: Notifying Customers Upfront and Ongoing Communication

- Provide upfront notice of potential robocall-related mitigations at onboarding and when changes occur.
- Deliver timely alerts about major mitigations that may affect call availability or quality.
- Offer contact channels for customer support, exception handling, and feedback.
- Publish an annual summary of remediation outcomes and improvements.

Step 6: Governance, Auditing, and Continuous Improvement

- Log all remediation actions with immutable records (who, when, what, why, outcome).
- Conduct periodic audits of data quality, policy adherence, and outcome effectiveness.
- Implement a formal improvement Plan (lessons learned, updated controls, and roadmap).