

Robocall Mitigation Program for 423 Communication, LLC

Even without STIR/SHAKEN, the company employs strong safeguards to prevent illegal robocalling.

4.1 Know-Your-Customer (KYC) Procedures

All customers are fully verified before enabling outbound calling.

Verification steps include:

- Legal business registration validation
- Physical address verification
- Ownership/beneficial owner identification
- Review of intended calling use cases
- Assessment for potential fraud or deceptive patterns
- Screening against known robocall offenders and high-risk lists

No customer receives service until verification is complete.

4.2 Ongoing Traffic Monitoring and Analytics

423 Communication, LLC continuously monitors outbound calling behavior using automated tools and manual review.

Monitored indicators include:

- High-volume, short-duration traffic bursts
- Calls to sequential or random number patterns
- Sudden changes in traffic behavior
- Excessive failed call attempts
- Calling profiles consistent with illegal telemarketing or fraud
- Overuse of CNAM or suspicious caller ID behavior

Alerts generate immediate investigation.

4.3 Handling Suspected Illegal Robocall Traffic

If suspicious traffic is detected:

1. Traffic is immediately **blocked or rate-limited**
2. The customer is contacted and required to verify call sources
3. A compliance investigation is opened
4. If misuse is confirmed, service is **terminated**
5. Relevant authorities may be notified (if necessary)

423 Communication, LLC maintains call logs and evidence for regulatory compliance.

4.4 Cooperation With Law Enforcement & ITG Tracebacks

423 Communication, LLC fully cooperates with the **Industry Traceback Group (ITG)** and law enforcement.

- All traceback requests are answered **within 24 hours**
- Detailed call records and routing information are provided
- Customer identity information is disclosed when legally permissible

The company maintains complete transparency in traceback investigations.

4.5 Network Security & Call Integrity Measures

To prevent spoofing and malicious traffic:

- SBCs enforce strict SIP header validation
- Invalid or unassigned number ranges are blocked
- Geographic and destination pattern controls
- Call rate limits for high-risk accounts
- TLS signaling (when supported by carriers)
- Unusual patterns trigger automated mitigation actions

All call detail records (CDRs) are retained for regulatory auditing.

4.6 Complaints Handling Procedure

If a carrier, regulatory agency, law enforcement entity, or consumer submits a complaint about suspected illegal robocalling:

1. Complaint Logging

- All complaints are documented in the internal compliance system.
- A timestamp, source, and summary of the issue are recorded immediately.

2. Initial Investigation (Within 24 Hours)

- Call records (CDRs), SIP logs, and account information are reviewed.
- Traffic behavior for the affected time period is analyzed.
- The customer associated with the traffic is contacted for clarification.

3. Decision & Mitigation

- If the call activity is legitimate and verified, the case is closed.
- If the traffic raises concern, outbound calling is **paused, limited, or blocked** pending further review.
- If the investigation confirms illegal or abusive calling, service is permanently **terminated**.
- When appropriate, the complaint information is shared with law enforcement or relevant authorities.

4. Documentation

- All actions taken are documented for FCC compliance and future audits.
-

4.7 Traceback Cooperation Statement

423 Communication, LLC **fully cooperates with all traceback requests** from the Industry Traceback Group (ITG), carriers, law enforcement, and regulatory authorities.

Traceback Response Commitment

- **We respond to *any* traceback request promptly—within 24 hours or sooner.**
- Detailed call path information, SIP signaling data, and customer identity (when legally allowed) are provided.
- The company maintains a dedicated compliance contact for traceback operations.
- 423 Communication, LLC does not obstruct, delay, or limit any traceback investigation.
- Internal processes ensure immediate retrieval of CDRs, routing logs, and account documentation to support the requesting authority.

This cooperation ensures alignment with FCC expectations and industry best practices for combatting illegal robocalls.