

Robocall Mitigation Plan – Elevate IT Solutions

Summary

- Company: Elevate IT Solutions
- Current controls: STIR/SHAKEN, reputation feeds, ML scoring, basic rate limiting
- Priorities: minimize false positives, aggressive blocking when necessary, regulatory compliance, good customer experience, cost control
- Timeline: immediate rollout with 90-day stabilization

1. Ownership & Core Team

- Executive Sponsors: Zach Walls, Connor Stafford
- Core Team: Network/VoIP Engineers, Security, Legal/Compliance, Customer Support, Data/Analytics
- On-call rotation: Connor Stafford, Cody Montgomery

2. Objectives & KPIs

- STIR/SHAKEN attestation pass rate $\geq 98\%$ for originating calls
- False-positive rate $< 0.5\%$ (legitimate calls incorrectly blocked)
- Complaint rate ≤ 1 per 10k calls
- Time to detect & mitigate new campaign ≤ 2 hours
- Time to resolve customer appeal ≤ 4 hours (business hours), ≤ 24 hours otherwise

3. Baseline actions (immediate, Day 0–3)

- Record current monthly call attempts, peak CPS, top 50 originating numbers per customer.
- Confirm STIR certificate validity and SBC attestation insertion for all origination trunks.
- Ensure ingestion of all reputation feeds into scoring; verify ML model health and last retrain date.

- Validate logging pipeline: call metadata, attestation result, score, action, and appeal ID stored centrally.

4. Per-customer traffic policy

- Default per-customer CPS limit: 1 CPS sustained; burst allowance: 10 calls in any 2-second window, 60 calls/minute for short bursts.
- High-volume customers: require pre-approved profile; otherwise enforce stricter limits (0.2 CPS sustained).
- Calls-per-day soft threshold: alert at 5,000 calls/day per customer; hard block at 10,000/day without verified business use.
- Automatic temporary throttling on anomaly (CPS spike > 3x baseline for that customer) — notify customer & fraud ops.

5. Scoring & handling rules

- Inputs: STIR attestation, ANI reputation, calling pattern (CPS, sequential ANIs), call duration, customer profile, geo mismatch, ML score.
- Actions by composite score:
 - Allow: low risk
 - Tag (notify recipient + label): medium risk
 - Challenge (IVR consent or SIP challenge): high risk
 - Block: very high risk
- Progressive policy: tag → challenge → block if repeated within rolling 24-hour window.
- Provide SIP reason headers and CDR flags to aid troubleshooting.

6. Provisioning & number controls

- Strengthened KYC for new customer/number orders: business registration, contact person, intended call profile, payment & credit checks.
- Mandatory traffic profile for any customer requesting >1 CPS or >5k/day.

- Porting: require documented authorization and 24-hour manual review for suspicious ports.
- Reserve right to suspend provisioning pending investigation.

7. Customer experience & appeals

- Customer UI/portal: report blocked calls, view blocked-call logs, request whitelist/appeal.
- Automated appeal intake with ticket created linking call logs, target response SLA above.
- Fast-track whitelist for verified legitimate business senders (temporary tokens, monitored).
- Notify customers immediately when their calls are challenged/blocked (email + portal message) with remediation steps.

8. Incident response & escalation

- Detection → Fraud Ops triage → Mitigate (throttle/block) → Notify customer & upstream carriers → If criminal, contact law enforcement → Postmortem within 72 hours.
- Maintain incident template: timeline, root cause, actions, affected customers, metrics, remediation.
- For major campaigns affecting multiple customers, engage carriers and file FCC/TCPA documentation as needed.

9. Monitoring, alerts & reporting

- Real-time dashboards: CPS (global & per-customer), blocked calls, STIR pass/fail, top blocked ANIs, customer complaints.
- Alerts:
 - CPS spike (global or per-customer) > 3x baseline → immediate page to on-call.
 - STIR failure rate > 2% → Ops alert.
 - Customer complaint > 1 in 10k calls → review.
- Weekly executive report and daily operational summary during active incidents.

10. Vendor & carrier coordination

- Maintain 2+ reputation feeds and one backup.
- Require vendor transparency on blocking criteria and notification of model changes.
- SLA with upstream carriers for rapid escalation (response within 2 hours during incidents).

11. Compliance & logging

- Retain call metadata and attestation logs for minimum 180 days (adjust per legal counsel).
- Document all mitigation actions for regulatory audits and law enforcement.
- Legal review of policies to ensure TCPA compliance and consumer privacy protections.

12. Testing & validation

- Canary rollout: new rules apply to 10% traffic (or to non-critical customers) first; monitor false positives for 48 hours.
- Monthly simulated attack tests to validate detection and throttle thresholds.
- Quarterly review of ML model performance and retrain if degradation observed.

13. Quick configuration examples

- Per-customer SIP trunk rate-limit: 1 CPS sustained, burst 60 calls/minute, block on sustained >3 CPS for 60s.
- Alert rule: page on-call if any customer exceeds 3x baseline CPS for 60s.

14. Continuous improvement

- Weekly review of blocked call samples and appeals; adjust rules to keep false positives <0.5%.
- Share anonymized intelligence with upstream carriers and industry groups.
- Quarterly policy and vendor performance review.