

Robocall Mitigation Program (RMP)

Partial STIR/SHAKEN Implementation — Non-Gateway Provider

Company	[E-Complish, LLC]
Provider Type	☐ Originating Voice Service Provider Non-Gateway Intermediate Provider (x)
Effective Date	[20250304]
Version	1.0
Approved By (Officer)	Gregory Gaines / COO

This document is intended as an internal operating policy and a source for the FCC Robocall Mitigation Database (RMD) narrative language. Replace bracketed placeholders before adoption.

1) Purpose

This Robocall Mitigation Program (“RMP”) establishes controls to prevent, detect, investigate, and stop illegal robocall traffic associated with E-Complish’s services, including operational processes required to meet caller ID authentication obligations and to respond to traceback inquiries within required timeframes.

2) Scope

- All voice services that originate, carry, or process calls on E-Complish’s network (including SIP trunks, hosted voice, UCaaS, resale arrangements, and interconnections).
- All call paths where E-Complish can perform STIR/SHAKEN and all call paths where it cannot (e.g., legacy/non-SIP segments, vendor limitations, incomplete SBC integration, hosted platform constraints).
- All employees and vendors involved in provisioning, routing, fraud/abuse monitoring, customer onboarding, and compliance.

3) Regulatory Commitments (Non-Gateway)

E-Complish commits to:

- Maintain an appropriate robocall mitigation program and certify accurately in the FCC Robocall Mitigation Database (RMD) where required.
- Respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the registered traceback consortium, and cooperate to investigate and stop illegal robocallers using our service.
- Implement caller ID authentication requirements for SIP calls to the extent required and technically feasible; where authentication is partial, apply the compensating controls described in this RMP.

4) Governance, Contacts, and Escalation

- RMP Owner (Marc Hopkins / Vice President of Strategic Relations)
- Compliance Lead: (Gregory Gaines / COO)
- 24/7 Traceback Contact (Required): [Angela Gregory agregory@e-complish.com | |888/847-7744 ext 208 | Rotational]
- NOC/Abuse Desk: [abuse@... / noc@...] (24/7 monitored)
- Escalation: Tier 1 (NOC) → Tier 2 (Fraud/Compliance) → Tier 3 (Officer)

Policy: Traceback intake channels must be monitored 24/7 to support the 24-hour response obligation.

5) STIR/SHAKEN Status: Partial Implementation

5.1 Partial Deployment Statement

E-Complish has a partial STIR/SHAKEN implementation, meaning:

- Authentication/verification is performed on some SIP call paths and network segments; and
- Certain call paths cannot yet be authenticated/verified due to documented constraints (e.g., non-SIP/TDM segments, vendor limitations, incomplete SBC integration, multi-tenant hosted platform constraints).

5.2 What We Do Today (Minimum Operational Requirements)

For SIP calls on segments where E-Complish controls the relevant network elements:

- Authenticate (sign) outbound calls that we originate where required.
- Verify authenticated caller ID information on inbound SIP calls that we terminate and/or pass onward, as applicable to our role.

5.3 Call Authentication Integrity Control

If E-Complish certifies partial (or complete) STIR/SHAKEN implementation in the RMD, E-Complish maintains its own required registrations/credentials and does not rely on third-party signing in a manner inconsistent with FCC caller ID authentication rules.

Operational note: We own our authentication posture, track signing/verification failures, and do not represent coverage beyond what we can operationally support.

5.4 STIR/SHAKEN Coverage Map (Required Internal Artifact)

Maintain and keep current an internal coverage table including: call path/segment name; can sign (Y/N); can verify (Y/N); traffic %; owner (network/vendor); and target date to enable (if N).

6) Roadmap to Expand from Partial to Full Coverage

E-Complish maintains a rolling roadmap with:

- Specific network elements to upgrade/integrate (e.g., SBC clusters, softswitches, hosted platforms).
- Vendor work items and target dates.
- Testing and cutover plan.
- Monitoring plan for authentication failure rates.

Minimum requirement: roadmap reviewed at least monthly by Compliance and Network leadership; exceptions are documented.

7) Compensating Robocall Controls for Non-Authenticated Segments

Where a segment cannot be authenticated/verified, E-Complish applies risk-based controls to prevent illegal traffic.

7.1 Caller ID Governance Controls

- Block or restrict clearly invalid caller ID patterns (invalid NANP formats, malformed From/P-Asserted-Identity values, etc.).
- Require evidence of right-to-use for customer-provided caller IDs (LOA/assignment evidence or other verification) for higher-risk customers/routes.
- Enforce caller ID whitelisting for high-volume customers where feasible.

7.2 Volume Management (CPS / Daily Attempts)

Definitions used for volume management:

- Busy Hour Average CPS (BH-Avg CPS): average call attempts per second during the busiest continuous 60 minutes in a rolling 24-hour window.
- Peak CPS: maximum call attempts per second measured over a defined interval (1-second or 5-second; select one and document).
- Daily attempts: total call attempts over a rolling 24-hour window.

Default caps for new/high-risk customers (example starting policy):

- Tier 1 (low risk): BH-Avg 10 / Peak 30 / Daily 100,000
- Tier 2 (medium): BH-Avg 5 / Peak 15 / Daily 50,000
- Tier 3 (high): BH-Avg 1 / Peak 3 / Daily 10,000

Caps increase only after a stability window (7–30 days) with clean performance and responsive compliance.

7.3 Tripwires (Contain First, Investigate Second)

Immediate containment (rate-limit/block/suspend) occurs when:

- Peak CPS exceeds 2× declared/approved peak for more than 5 minutes.
- BH-Avg CPS exceeds 150% of approved BH average.
- Daily attempts exceed 120% of cap.
- High-rotation caller ID behavior or repeated short-duration burst signatures are detected.
- A traceback request ties suspicious traffic to an active customer/trunk.

All actions are ticketed with reason codes and approvals.

8) Know-Your-Customer (KYC) and Know-Your-Upstream (KYUP)

8.1 KYC (Outbound-Enabled Customers)

Before enabling outbound calling (or scaling volume), collect and retain:

- Legal entity validation and authorized users.
- Use-case description (campaign type, scripts, target geographies, calling windows).
- Compliance attestation (e.g., TCPA/TSR where applicable).
- Caller ID authority evidence.
- Expected CPS/daily volume and destinations.
- Escalation contacts and abuse response commitment.

8.2 KYUP (Upstream Interconnects)

For each upstream provider/interconnect, maintain:

- Contract clauses: anti-robocall obligations, traceback cooperation, immediate mitigation rights.
- 24/7 abuse/traceback contact paths.
- Traffic profile expectations with caps and tripwires.
- Ongoing monitoring and periodic re-validation.

9) Monitoring, Analytics, Blocking, and Enforcement

9.1 Analytics and Monitoring (Always-On)

Monitor per customer/trunk:

- Burst/spike patterns (CPS and daily volume).
- Low ASR/low ACD/high short-duration ratios.
- Caller ID anomalies and unusual rotation.
- Complaint signals (carrier feedback, consumer complaints relayed, downstream notices).

9.2 Tools and Vendors

- Primary analytics platform(s): [Vendor/Tool]
- SBC/firewall controls: [Vendor/Tool]
- Ticketing/case management: [Tool]

9.3 Enforcement Actions

Depending on risk, E-Complish may block calling numbers/prefixes, rate-limit by customer/trunk, require documentation within a defined deadline, and suspend/terminate service for confirmed violations.

10) Traceback Response Playbook (24-Hour SLA)

10.1 Intake Channels

- Primary: traceback@E-Complish.com (24/7 monitored)
- Secondary: [on-call phone/pager]
- Tracking: [ticket system]

10.2 Standard Procedure

- Acknowledge receipt (target: <2 hours).
- Identify call path (customer/trunk/upstream).
- Provide requested artifacts (CDRs, timestamps, SIP headers where available).
- Apply containment if tripwires indicate ongoing risk.
- Preserve evidence.
- Close the loop with requester (actions taken and disposition).

Commitment: respond within 24 hours and cooperate to stop illegal robocallers.

11) Recordkeeping and Retention

Maintain:

- KYC/KYUP files and contracts.
- STIR/SHAKEN coverage map and roadmap.
- Monitoring alerts, enforcement tickets, approvals.
- Traceback requests/responses and evidence produced.
- Certificate/signing/verification operational logs (where applicable).

Retention: [24 months] minimum (or longer if law/contract requires).

12) RMD Operations Note

If E-Complish is an RMD filer, E-Complish maintains accurate certifications, including whether STIR/SHAKEN is partial vs. complete and what mitigation controls apply to non-authenticated segments.

Appendix A — RMD-Ready Narrative (Partial STIR/SHAKEN)

Robocall Mitigation Program Summary (Partial STIR/SHAKEN):

E-Complish maintains a written Robocall Mitigation Program to prevent illegal robocalls. E-Complish has partial STIR/SHAKEN and authenticates/verifies SIP calls where it controls the elements. For non-authenticated call paths, E-Complish uses compensating controls including

KYC/KYUP, CPS/daily caps, traffic analytics, caller ID governance, and enforcement actions. E-Complish responds within 24 hours to traceback requests.