

FCC ROBOCALL MITIGATION PLAN

Filing Entity Information

Provider Name: Bergman Consulting Services, LLC

FRN: 0038022760

Provider Classification:

Voice Service Provider without a STIR/SHAKEN implementation obligation

1 Provider Role and Network Architecture

The filing entity operates as a non-facilities-based hosted VoIP service provider delivering voice services to end users through upstream voice service providers that control transmission facilities and call origination infrastructure.

The filing entity:

- Does not operate its own PSTN switching infrastructure
- Does not independently originate calls at the network signaling layer
- Does not possess an STI certificate or perform STIR/SHAKEN signing
- Lacks control over the network infrastructure necessary to implement STIR/SHAKEN

Therefore, the filing entity has no independent STIR/SHAKEN implementation obligation under FCC rules.

2 Regulatory Compliance Framework

The filing entity maintains a robocall mitigation program designed to meet the “reasonable steps” standard defined in:

47 CFR §64.6305(a)

The program is intended to prevent, detect, and mitigate illegal robocall traffic originating from customers using its services.

Customer Due Diligence and Risk Management

Identity Verification

Prior to activation of services, the filing entity performs customer vetting including:

- Verification of business or individual identity
- Review of intended use case and calling practices
- Collection of contact and billing information

Risk-Based Screening

The filing entity evaluates customers for risk indicators including:

- High-risk vertical markets
- High-volume outbound dialing profiles
- Indicators associated with known abuse patterns

Contractual Controls

Customer agreements include:

- Prohibitions on illegal robocalling and spoofing
 - Compliance with applicable telemarketing and consent laws
 - Authorization for monitoring and enforcement actions
-

Traffic Monitoring and Abuse Detection

The filing entity maintains operational procedures to identify suspicious traffic patterns, including:

- Abnormal call volume increases
- High short-duration call ratios
- Excessive call failure rates
- Complaint-driven investigations

When potential abuse is identified:

- Traffic is reviewed

- Customers may be contacted
 - Restrictions or blocking may be applied
 - Accounts may be suspended or terminated
-

5 Upstream Provider Reliance and Network Controls

The filing entity utilizes upstream providers that:

- Implement STIR/SHAKEN authentication
- Maintain robocall mitigation programs
- Provide network-level analytics and blocking capabilities

The filing entity relies on upstream authentication while maintaining independent mitigation responsibilities at the customer level.

6 Shared Responsibility Model and Call Chain Role

The filing entity operates within a multi-layered VoIP ecosystem in which robocall mitigation responsibilities are shared among downstream service providers, upstream originating carriers, intermediate providers, and terminating networks. The filing entity acknowledges its role as a downstream voice service provider serving end users while upstream providers control network-level authentication, call origination, and STIR/SHAKEN implementation.

The filing entity implements customer-facing mitigation controls designed to prevent unlawful traffic from entering the upstream network, while relying on upstream providers to apply authentication, attestation, analytics, and network-level blocking controls. This layered mitigation model reflects industry best practices and aligns with the Commission's expectations that each participant in the call chain take reasonable steps within their operational control to reduce illegal robocalls.

The filing entity understands that participation in this shared responsibility model requires ongoing coordination with upstream providers, adherence to traceback requirements, and proactive enforcement of acceptable use policies to prevent abuse of hosted VoIP services.

7 Know-Your-Upstream Provider Practices

The filing entity exercises reasonable diligence regarding upstream providers, including:

- Using reputable providers expected to maintain FCC compliance
 - Understanding upstream mitigation practices
 - Cooperating with upstream enforcement actions when necessary
-

8 Traceback and Law Enforcement Cooperation

The filing entity commits to:

- Respond fully within 24 hours to traceback requests from:
 - The Federal Communications Commission
 - Law enforcement agencies
 - The Industry Traceback Group

Mitigation actions may include:

- Traffic blocking
 - Account suspension
 - Termination of service
-

9 Call Analytics and Mitigation Tools

The filing entity relies on:

- Upstream call analytics systems
- Internal monitoring processes
- Industry best practices

Where applicable, mitigation actions may include filtering, blocking, or investigation of suspicious traffic.

10 Continuous Compliance and Program Governance

The filing entity periodically reviews:

- Mitigation procedures
- Customer risk profiles
- Regulatory updates
- Industry standards

The program evolves as necessary to address emerging robocall threats.

1 1 Certification Statement

The filing entity certifies that:

- Calls originating from customers are subject to this robocall mitigation program.
- The entity lacks control over network infrastructure necessary to implement STIR/SHAKEN.
- The entity complies with applicable FCC robocall mitigation rules.