

Robocall Mitigation Plan

Entity Name: VIRTUAL INTERNATIONAL HOLDINGS, INC.

DOS ID: 5766898

Business Address: 418 Broadway, Ste N, Albany, NY 12207, United States

CEO: Michael Ashlawn

Email: info@virtualinternationalholdings.com

Phone: 646-368-2536

1. Purpose

VIRTUAL INTERNATIONAL HOLDINGS, INC. (“Company”) has adopted this Robocall Mitigation Plan to prevent unlawful robocalls from originating on, passing through, or being transmitted using its voice services, and to comply with applicable requirements of the Federal Communications Commission (FCC) and related industry standards.

The Company commits to actively mitigate illegal robocall traffic and to implement procedures designed to identify, investigate, block, and prevent unlawful call activity.

2. Scope

This plan applies to:

- Outbound voice traffic originated by the Company or its customers
- Inbound and transit voice traffic handled by the Company
- Domestic and international interconnected voice services, including VoIP services, where applicable
- All customers, resellers, and upstream/downstream provider relationships

3. STIR/SHAKEN Implementation Status

The Company:

- Has implemented or is implementing STIR/SHAKEN authentication where technically feasible and required.
- Authenticates caller ID information for calls originated on its network.

- Verifies and validates caller ID information received from interconnected providers.
- Uses attestation levels (A, B, or C) as appropriate based on customer and number verification.

Where full STIR/SHAKEN implementation is not feasible for portions of the network, the Company applies the mitigation practices described below.

4. Robocall Mitigation Practices

The Company uses the following mitigation measures:

A. Know-Your-Customer (KYC) Procedures

Before providing service, the Company verifies:

- Customer legal identity
- Business registration information
- Authorized use of telephone numbers
- Nature of intended calling activity
- Compliance representations regarding lawful traffic

High-risk customers may undergo enhanced due diligence.

B. Traffic Monitoring

The Company monitors for suspicious patterns, including:

- Unusually high call volumes
- Short-duration or burst traffic
- Neighbor spoofing
- Invalid, unallocated, or spoofed caller IDs
- Repeated consumer complaints
- Patterns associated with illegal robocall campaigns

C. Call Analytics and Blocking

The Company may use:

- Reputation-based analytics

- Automated suspicious call detection
- Blocking of clearly unlawful traffic
- Traceback response data
- Number validation tools

D. Customer Enforcement

If suspicious or unlawful traffic is detected, the Company may:

- Suspend or block traffic
- Require remediation from customers
- Terminate service
- Report unlawful activity to appropriate authorities

5. Response to Traceback Requests

The Company agrees to:

- Respond promptly to traceback requests from the Industry Traceback Group or authorized partners
- Investigate identified traffic sources
- Cooperate with law enforcement and regulators when appropriate
- Maintain records of traceback responses

6. Spoofing Prevention

The Company prohibits:

- Transmission of knowingly false or misleading caller ID information
- Unauthorized number spoofing
- Use of invalid or unassigned numbers
- Traffic that violates the Truth in Caller ID Act

7. Recordkeeping

The Company maintains records related to:

- Customer onboarding and due diligence
- Traffic monitoring activities
- Robocall investigations
- Traceback responses
- Enforcement actions
- Compliance reviews

Records are retained according to applicable legal and regulatory requirements.

8. Vendor and Upstream/Downstream Provider Oversight

The Company evaluates providers and partners through:

- Contractual compliance provisions
- Traffic integrity monitoring
- Provider due diligence
- Review of known high-risk traffic sources

The Company may cease doing business with providers linked to unlawful traffic.

9. Internal Compliance Oversight

Compliance responsibility is assigned to management under the oversight of the CEO.

Responsible functions include:

- Monitoring compliance with this plan
- Reviewing suspicious traffic reports
- Updating mitigation procedures as risks evolve
- Maintaining FCC Robocall Mitigation Database information

10. Employee Training

Relevant personnel receive training concerning:

- Illegal robocall indicators
- Traceback handling procedures
- Traffic monitoring protocols

- Escalation procedures
- Regulatory obligations

11. Review and Updates

This plan is reviewed at least annually and updated when:

- FCC requirements change
- Network architecture changes
- New robocall risks emerge
- Material compliance events occur

12. Certification

VIRTUAL INTERNATIONAL HOLDINGS, INC. certifies it has implemented measures to mitigate illegal robocalls and will continue to take reasonable steps to prevent unlawful traffic on its network.

Authorized Representative: Michael Ashlawn, CEO

Entity: VIRTUAL INTERNATIONAL HOLDINGS, INC.

Date: 22/04/2026