

Heimdall Strategy Robocall Mitigation Plan

Last Updated: 12/19/2024

1. Introduction & Purpose

Heimdall Strategy, Inc. ("the Company") is dedicated to preventing and mitigating illegal robocall traffic originating on its network. In accordance with the FCC's Public Notice DA 24-73A1, this Robocall Mitigation Plan details the Company's methods, policies, and procedures for identifying and eliminating unlawful calls, ensuring compliance with the TRACED Act, the FCC's Call Authentication Trust Anchor (CATA) requirements, and the STIR/SHAKEN caller ID authentication framework.

This Plan will be implemented throughout the Company's voice service operations to:

- Reduce the origination and transit of illegal robocalls.
- Confirm legitimate traffic sources through robust customer vetting.
- Cooperate with industry traceback requests and enforcement actions.
- Comply with all relevant state and federal regulations governing robocall mitigation.

2. Implementation of STIR/SHAKEN Caller ID Authentication

2.1 Compliance Status

Heimdall Strategy is using a provider that has implemented STIR/SHAKEN protocol standards across all IP-based voice networks. STIR/SHAKEN is used to verify caller identity and to authenticate the legitimacy of calls that traverse our network.

2.2 Non-IP Networks

Heimdall Strategy does not use any Non-IP networks.

3. Customer Vetting & Onboarding Procedures

3.1 Know-Your-Customer (KYC) Protocols

Before onboarding new customers (such as voice service resellers, enterprise clients, or high-volume calling platforms), Heimdall Strategy performs rigorous KYC checks, which include:

- Confirming the customer's identity and legal status (e.g., business registration, licensing).
- Reviewing the customer's intended use-case for call traffic.
- Obtaining formal attestations that the customer will not engage in illegal robocalling practices.

3.2 Traffic Profile Establishment

Upon establishing a business relationship, Heimdall Strategy sets a baseline traffic profile for each customer (e.g., call volume, call duration, call destinations). Subsequent variations are monitored to detect anomalies that may indicate illegal activity.

4. Ongoing Monitoring & Traffic Analysis

4.1 Automated Monitoring Tools

Heimdall Strategy employs automated analytics and machine-learning-based tools to monitor network traffic in real-time. Suspicious calling patterns—such as high short-duration call volumes to sequential or unassigned numbers—trigger alerts for further investigation.

4.2 Call Detail Record (CDR) Review

The Company reviews CDRs to identify spikes in call attempts, abnormal calling hours, or other red flags. Enhanced analytics platforms compare observed traffic against known patterns of illegal robocalling to inform mitigation measures.

4.3 Blocking and Labeling

When suspicious activity is detected, Heimdall Strategy may:

- Temporarily block outbound calls from the offending source.
- Insert call labeling (e.g., “Spam?” or “Potential Fraud”) into caller ID fields to alert call recipients.
- Escalate the matter internally for immediate human review and potential termination of the offending customer’s services.

5. Industry Cooperation & Call Traceback Support

5.1 Participation in Traceback Initiatives

Heimdall Strategy collaborates with the Industry Traceback Group (ITG) and other FCC-recognized traceback consortiums. Upon receiving a traceback request, the Company promptly investigates and supplies the requested call records or relevant information, consistent with legal requirements.

5.2 Reporting & Escalation

Heimdall Strategy promptly reports suspicious traffic to the FCC and other appropriate enforcement authorities. The Company maintains direct contact points to facilitate timely communication and resolution of issues.

6. Enforcement Actions Against Customers Originating Illegal Robocalls

6.1 Warning & Compliance Notices

If a customer’s traffic is found to be generating illegal robocalls, Heimdall Strategy issues a formal warning, requiring immediate remediation and a demonstration of compliance within a specified timeframe.

6.2 Service Suspension or Termination

Should a customer fail to cease illegal robocalling practices, Heimdall Strategy may suspend or terminate the customer’s service. We maintain clear contractual provisions allowing service termination for non-compliance with telemarketing and robocall laws.

7. Publicly Accessible Information & Robocall Mitigation Database

7.1 Database Filing

Heimdall Strategy will file its Robocall Mitigation Plan and other required certifications with the FCC’s Robocall Mitigation Database, as mandated. We will ensure that the most current version of this Plan is publicly accessible and that any material changes are promptly reflected and reported.

7.2 Public Documentation

A summary of our Robocall Mitigation practices, including STIR/SHAKEN implementation status and essential mitigation steps, will be made available on the Company's website. This ensures transparency and compliance with public disclosure requirements.

8. Training & Internal Controls

8.1 Employee Training

All relevant staff receive periodic training on robocall mitigation techniques, STIR/SHAKEN implementation, traceback procedures, and compliance obligations. Employees are encouraged to report suspicious activity through established internal channels.

8.2 Continuous Improvement

The Company regularly updates its mitigation strategies to reflect evolving best practices, guidance from regulatory authorities, and new technical solutions. Periodic internal audits and external reviews ensure the effectiveness of the Plan.

9. Compliance Oversight & Contact Information

9.1 Compliance Officer

Heimdall Strategy designates a Compliance Officer responsible for overseeing the implementation of this Plan, monitoring compliance metrics, and reporting status updates to executive leadership.

9.2 Contact Information

For any inquiries related to this Robocall Mitigation Plan, contact:

Name/Title: Jefferson Nunn, CTO

Email: jefferson@heimdallstrategy.com

Phone: 817-666-2444

Signature & Attestation

I, the undersigned, attest that Heimdall Strategy has implemented the above Robocall Mitigation Plan and will abide by the procedures, obligations, and commitments herein, to the best of our ability and knowledge.

Jefferson Nunn

CTO

Heimdall Strategy

Date: 12/19/2024