

STIR/SHAKEN Implementation

CloudNetix ("Company") is a service provider offering secure, scalable voice solutions to commercial and carrier markets. CloudNetix's network solutions are designed to help customers control, scale, and improve business value through the use of innovative cloudbased platforms and next-generation network services. CloudNetix has implemented STIR/SHAKEN and has certified that all voice traffic originating on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. §64.6301(a).

Depending on the services provided, CloudNetix may serve as a Voice Service Provider, Gateway Provider, and/or Non-Gateway Intermediate Provider. As such, CloudNetix submits this Robocall Mitigation Program ("RMP") and certification into the Robocall Mitigation Database. This RMP includes the obligations outlined in the Commission's release, In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (rel. March 17, 2023).

ROBOCALL MITIGATION Background

The FCC Order requires that an RMP include the following affirmative obligations for voice service providers:

- Outline reasonable steps taken to avoid originating illegal robocall traffic.
 - Commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium, and to cooperate with such entities.
 - Know Your Customer (KYC) procedures.
 - Description of call analytics systems used to identify and block illegal traffic.
-

Traceback

CloudNetix is committed to ensuring its network is not used for the origination or termination of illegal robocalls. CloudNetix will respond fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group ("ITG"), and will cooperate

with such entities in investigating and stopping any illegal robocallers that use its services. CloudNetix complies with ITG policies and procedures.

If patterns of suspicious calls are identified, CloudNetix will open a case with the customer. In extreme cases, the Company may suspend the customer's ability to transit traffic until issues are investigated and resolved.

Traceback Contact Information

Name: Peter Koch

Title: Compliance Officer

Email address: contact@CloudNetix.com

Call Blocking/Analytics for Monitoring Traffic

CloudNetix has implemented analytics systems to identify unlawful traffic that may originate on its network. These systems include statistical analysis, velocity analysis, and computational methods to detect and mitigate illegal robocalls.

- Real-time lookup systems detect invalid, unallocated, or Do Not Originate (DNO) numbers.
- Calls detected as unlawful are blocked, and reports are generated for investigation.
- CloudNetix monitors the Robocall Mitigation Database to confirm traffic only originates from registered carriers.

Know Your Customer Protocols

CloudNetix has implemented effective KYC measures to prevent new and renewing customers from using its services to originate illegal robocalls. These protocols include:

- Initial Contact: Collection of customer's legal name, incorporation documents, address, billing details, federal tax ID, and nature of business.
- Document Verification: Government-issued IDs, utility bills, and other corporate documents are required.
- Know Your Traffic: Additional traffic compliance documentation may be requested.
- Risk Profiling: Assessment of customer's risk level based on services requested, business model, and compliance history.

- **Monitoring:** High-risk customers are subject to heightened monitoring and periodic reviews.
 - **Compliance Checks:** Regular screening against local and international watchlists.
-

Validating Customer's Right to Use Numbers

CloudNetix requires that all telephone numbers are either directly assigned by the Company or ported-in under regulated processes. Proper tracking and inventory systems ensure number use is valid and authorized.

Accepting Traffic From Other Providers

- **Domestic Providers:** Calls are only accepted from domestic providers listed in the FCC RMD and not de-listed.
 - **Foreign Providers:** Calls are only accepted from foreign providers listed in the RMD and not de-listed.
 - **Gateway Providers:** Calls are only accepted from gateway providers affirmatively registered and active in the RMD.
 - **Emergency Services:** Calls to 911, PSAPs, and government emergency numbers are never blocked.
-

Authenticating Voice Traffic

In accordance with 47 C.F.R. §64.6301(a), when operating as a Voice Service Provider, CloudNetix authenticates and verifies originator identification for SIP calls on its network, transmitting authenticated caller ID information to subsequent providers. When operating as a Gateway or Intermediate Provider, CloudNetix authenticates caller ID information for all calls it receives using U.S. numbering resources before exchanging them with other providers.

Acceptable Use Policy

CloudNetix's Terms and Conditions outline permissible service use, prohibiting illegal activity, fraud, and generation of unlawful robocalls. The Company may pause, suspend, or terminate service to customers violating these terms.

Company Information

Company Name: CloudNetix

Phone: 1 877 212 7021

Address: 29805 US Highway 24

Buena Vista, CO 81211-9640

United States

Designated Contact: Melissa Brooks

Email: contact@CloudNetix.com

Conclusion

This Robocall Mitigation Program is submitted consistent with FCC regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). CloudNetix will update its submission in the RMD within 10 business days of any material change, including updates to this RMP. CloudNetix remains committed to protecting consumers and ensuring its services are not used for unlawful robocall traffic.