



At Sinistra, we are devoted to creating a secure and reliable communication environment for our clients by proactively combating the growing concern of robocalling. Our Robocall Prevention Strategy (RPS) is designed to implement cutting-edge technology, align with federal regulations, and ensure a fraud-free network for all users. By adopting a multi-layered approach to robocall prevention, we provide businesses with a trusted and compliant communications platform.

Strategic Goals

1. Regulatory Adherence:

We are committed to adhering to all relevant legal standards, including the Federal Communications Commission (FCC) regulations and STIR/SHAKEN protocols, to ensure that our operations remain free from robocall-related issues and uphold industry best practices.

2. Protection of Client Communications:

Sinistra aims to safeguard all customer communications by preventing fraudulent calls, ensuring that every interaction on our network is authentic, safe, and secure.

3. Continuous Improvement:

Our strategy includes an ongoing process of innovation and refinement to enhance our prevention systems and minimize the risk of robocalling, helping businesses maintain trust with their clients and customers.

Robocall Prevention Measures

1. Comprehensive Traffic Surveillance

We employ advanced traffic monitoring tools to analyse call data, including call patterns, duration, and frequency. This allows us to detect irregularities in traffic and identify suspicious activity early, effectively preventing robocall threats.

2. Rigorous Origin Verification and ANI Scrutiny

Sinistra implements robust checks for both traffic origins and Automatic Number Identification (ANI) for all calls made through our services. By verifying caller information and blocking suspicious or unauthorized sources, we minimize the chances of robocalls infiltrating our network.

3. Strict Enforcement Against Malicious Callers

We operate under a zero-tolerance policy for illegal robocalling. Any client found violating our terms through fraudulent practices or involvement in robocalling will face immediate consequences, including suspension or termination of their service.

4. Client and Caller ID Verification

All new clients undergo comprehensive background checks and identity verification. This includes scrutinizing caller ID data and ensuring that all information meets our standards for legitimacy before allowing use of our network.



5. Partnership with Trusted Providers

Sinistra collaborates closely with upstream providers and other telecom operators to identify and mitigate robocalling risks as soon as they arise. This ensures a coordinated and rapid response to emerging threats, maintaining the integrity of our network.

6. Regular System Audits and Traceback Capabilities

We conduct routine system audits to detect any irregularities in our network that could be exploited for robocalling purposes. In the event of a potential fraud incident, we carry out a full traceback process to investigate the origin of suspicious calls and prevent further disruptions.

7. Prompt and Transparent Customer Communication

We maintain clear communication with our clients, particularly if unusual activity is detected. By working closely with businesses and their end-users, we quickly identify potential system issues or violations and ensure a swift resolution to minimize impact.

8. Full STIR/SHAKEN Integration

As a commitment to call authentication and fraud prevention, Sinistra fully integrates the STIR/SHAKEN framework. This industry-standard technology helps authenticate calls, preventing the spoofing of caller information and ensuring that calls on our network are trustworthy.

Conclusion

Sinistra Robocall Prevention Strategy is a comprehensive and proactive approach to combating the ongoing issue of robocalls. Through a combination of advanced monitoring, stringent verification, legal compliance, and transparent communication, we provide a secure platform for our clients to engage with their customers. We remain vigilant in protecting against malicious activities, continuously improving our systems to stay ahead of emerging threats.

By prioritizing security and transparency, Sinistra ensures that businesses can communicate effectively and ethically, free from the risks posed by robocalling and other fraudulent activities.

Sinistra LLC

FRN: 0036747897

FCC: 837473

www.sinistra.us

+1-334-403-6555