

02/26/2024

Federal Communications Commission
Washington, D.C. 20554
United States of America

Letter to the Commission

RE: FCC Robocall Mitigation Database (RMD) / Robocall Mitigation Plans (RMPs)

1. SIPSTACK Inc. ("SIPSTACK") submits this Robocall Mitigation Plan to the Federal Communications Commission ("FCC") in relation to the FCC's Robocall Mitigation Database ("RMD"). pursuant to 47 CFR § 64.6305(d).
2. SIPTACK is a Canadian registered telecommunications provider subject to the Canadian Telecommunications Act (S.C. 1993, c. 38) ("Telecom Act") and to the regulatory authority of the Canadian Radio-television and Telecommunications Commission ("CRTC"). For the purpose of its registration in the RMD, SIPSTACK is a foreign voice service provider.

Full Implementation of STIR/SHAKEN

3. SIPTACK has fully implemented the STIR/SHAKEN authentication framework across its network for all calls it carries or processes for US origination and termination in compliance with the requirements of Section 64.6302(b) of the Commission's rules including participation in the traceback process.

Robocall Mitigation Plan

4. SIPSTACK is dedicated to maintaining the highest level of network infrastructure security and safeguarding our customers from malicious activities, including hackers, spoofers, robocalls, robotexts, scams, and nuisance calls. To further this commitment, we have implemented comprehensive strategies and technologies that go beyond basic compliance requirements:
 - a. **Network-Level Blocking:** We've instituted advanced blocking strategies that automatically identify and prevent known fraudulent numbers or suspicious calling patterns from reaching our customers. This proactive approach is continuously refined based on emerging threats and patterns identified both internally and across the telecommunications industry.
 - b. **Industry Collaboration:** SIPSTACK actively participates in industry-wide initiatives to share intelligence about fraud and spam trends. By collaborating with other

providers and industry groups, we can leverage a collective knowledge base to better anticipate and combat new robocall tactics before they impact our network and customers.

- c. **Enhanced Customer Protection Tools:** In addition to our Smart CNAM service, we offer our customers a suite of tools and options to personalize their protection against unwanted calls. This includes customizable call blocking features, allowing customers to tailor their defense mechanisms according to their preferences and risk profiles.
- d. **Public Education and Awareness:** Recognizing the importance of informed customers in the fight against robocalls, we engage in ongoing public education efforts. These initiatives aim to raise awareness about the risks associated with robocalls and the measures individuals can take to protect themselves, thereby fostering a more resilient community.

Through these enhanced measures, SIPSTACK not only adheres to regulatory requirements but also demonstrates a proactive stance in protecting the integrity of our telecommunications services and the privacy of our customers.

- 5. SIPSTACK has deployed cutting-edge artificial intelligence (AI) and machine learning (ML) technologies across our network to significantly reduce the origination of illegal robocalls.

These technologies are central to our strategy, providing dynamic and adaptive solutions to detect and mitigate fraudulent calls in real-time. Here are the key components of our AI/ML deployment:

- a. **Real-Time Call Analysis and Anomaly Detection:** Our AI/ML models are trained on a vast dataset of call patterns, allowing for the immediate identification of anomalies that may indicate spam or fraudulent activity. By analyzing various aspects of calls, including their origin, frequency, and known scam indicators, our system can flag suspicious activities with high accuracy.
- b. **Dynamic Model Training and Updating:** The effectiveness of our AI/ML models depends on their ability to learn from new data. To this end, we continuously feed our models with the latest call data, including confirmed instances of fraud and feedback from our customer base. This ensures that our models evolve in response to the ever-changing tactics employed by bad actors.
- c. **Customer Feedback Loop:** We have implemented mechanisms for customers to report suspicious calls directly to us. This feedback is invaluable, as it helps to further train our AI/ML models with real-world data, ensuring that our mitigation strategies are aligned with the actual experiences of our users.
- d. **Transparency and Control for Customers:** Beyond just blocking suspicious calls, we provide our customers with insights into why certain calls were blocked or flagged. This transparency helps build trust and gives customers a sense of control over their communications.

Through these sophisticated AI/ML implementations, SIPSTACK is at the forefront of combating illegal robocalls, ensuring our network and our customers are protected with the

most advanced and effective technologies available.

6. SIPSTACK leverages Smart CNAM, an advanced AI/ML-powered lookup tool, alongside our proprietary technological innovations, to provide a comprehensive defense against illegal robocalls. These systems are integral to our robocall mitigation strategy, offering nuanced and effective measures to protect our network and customers:
 - a. **Smart CNAM in Action:** Utilizing artificial intelligence and machine learning, Smart CNAM performs real-time risk assessments of incoming calls. It evaluates various indicators of potential fraud, such as the call origin, frequency, and known scam patterns, to accurately flag suspicious activities. This tool is continuously updated to adapt to new tactics used by spammers and fraudsters, ensuring our defenses remain robust and responsive.
 - b. **Active FCC and Industry Engagement:** We maintain an active monitoring stance on FCC communications, guidelines, and advisories concerning illegal robocalls. This vigilance extends to our participation in industry forums and collaborations, where we share insights and learn from the collective experience of the telecommunications community to refine our strategies.
 - c. **Consumer Complaints Database Monitoring:** By closely analyzing the FCC's consumer complaints database, we gain valuable insights into the evolving landscape of robocall threats. This analysis informs the ongoing development of our AI/ML models, ensuring they are attuned to current and emerging patterns of illegal activity.
 - d. **Proprietary Method Enhancements:**
 - i. **Adaptive Learning Models:** Our proprietary methods include advanced adaptive learning models that go beyond standard AI/ML techniques. These models are specifically designed to detect and adapt to novel robocall strategies faster than conventional systems, providing an extra layer of security and responsiveness.
 - ii. **Custom Algorithm Development:** We have developed custom algorithms that enhance the predictive accuracy of our AI/ML systems. These algorithms are tailored to identify subtle patterns and anomalies in call data that might be overlooked by off-the-shelf solutions, allowing for more precise identification of potential threats.
 - iii. **Secure Data Integration:** In our quest to enhance the efficacy of Smart CNAM, we integrate secure, anonymized data from our network operations with external threat intelligence. This holistic approach enriches our data set, enabling our models to learn from a wider array of scenarios and apply these learnings to real-time call analysis.

Through the sophisticated application of Smart CNAM and our proprietary AI/ML innovations, SIPSTACK provides unparalleled protection against the scourge of illegal robocalls. Our commitment to continuous improvement and adaptation ensures that our network remains a hostile environment for fraudsters and spammers, safeguarding our customers' communication experiences.

Know Your Customer

7. At SIPSTACK, we understand the critical importance of thoroughly knowing our customers to prevent our services from being used for illegal robocalls. Our KYC procedures are designed to ensure a high level of due diligence for both new and existing customers, incorporating several layers of verification and ongoing monitoring:
 - a. **Initial Customer Vetting:**
 - i. **Documentation and Identity Verification:** New customers are required to provide comprehensive documentation, including business registration details, ownership information, and proof of identity for key contacts. This information is verified through trusted third-party databases to ensure authenticity.
 - ii. **Credit and Risk Assessment:** We conduct a thorough assessment of each new customer's credit history and potential risk factors. This includes evaluating their business activities, industry sector, and any previous telecommunications-related violations or complaints.
 - iii. **Regulatory Compliance Check:** Each new customer undergoes a regulatory compliance review to ensure they adhere to relevant telecommunications laws and regulations, both domestically and in their respective jurisdictions.
 - b. **Ongoing Customer Monitoring:**
 - i. **Regular Account Reviews:** Existing customers are subject to periodic reviews to ensure continued compliance with our policies and regulatory standards. This includes revisiting credit assessments, business activities, and any changes in ownership or key personnel.
 - ii. **Activity Monitoring and Alerts:** Our systems continuously monitor customer activities for patterns that may indicate a deviation from normal business operations or potential misuse of our services for robocall activities. Alerts are generated for any anomalies, triggering further investigation.
 - iii. **Customer Education and Engagement:** We actively engage with our customers to educate them about the importance of robocall mitigation and the role they play in preventing misuse of telecommunications services. This includes providing resources and best practices for identifying and reporting suspicious activities.
 - c. **Enhanced Due Diligence for High-Risk Customers:**
 - i. For customers identified as higher risk due to their business model, geography, or previous history of complaints, we implement enhanced due diligence measures. These may include more frequent reviews, additional documentation requirements, and closer monitoring of call traffic patterns.

Through these meticulous KYC procedures, SIPSTACK not only complies with regulatory requirements but also actively contributes to the broader effort to combat illegal robocalls. Our approach ensures that we maintain a trusted and secure telecommunications environment for all our customers, while vigilantly guarding against potential abuse.

Traceback Requests

8. SIPSTACK is committed to working and cooperating with our customers, partners, vendors and with regulatory and legal authorities to address issues, including assisting with traceback activities related to unlawful and non-compliant activities.

Know Your Upstream Provider

9. In our efforts to maintain the integrity of our network and protect our customers from illegal robocalls, SIPSTACK places significant emphasis on thoroughly understanding and vetting our upstream providers. Recognizing the crucial role these providers play in the telecommunications ecosystem, we have instituted comprehensive procedures to ensure they adhere to the highest standards of conduct and regulatory compliance.
 - a. **Vetting and Selection Process:**
 - i. **Regulatory Compliance Verification:** We conduct a thorough assessment of potential upstream providers' compliance with relevant telecommunications regulations and standards. This includes verifying their participation in industry-standard robocall mitigation efforts, such as STIR/SHAKEN.
 - ii. **Reputation and Reference Checks:** We perform checks on the reputation of potential upstream providers, including reference checks with other industry participants and reviewing any public records of regulatory violations or consumer complaints.
 - b. **Ongoing Monitoring and Review:**
 - i. **Performance and Compliance Monitoring:** Once onboarded, our upstream providers are subject to continuous monitoring to ensure they maintain the required standards of service quality and regulatory compliance. This includes reviewing any updates to their robocall mitigation strategies and practices.
 - ii. **Regular Audits and Assessments:** We conduct regular audits of our upstream providers to verify ongoing compliance with our contractual agreements and operational expectations. These audits are designed to identify any potential areas for improvement in robocall mitigation efforts.
 - c. **Mitigation of Non-Compliant Providers:**
 - i. In cases where an upstream provider fails to meet our standards or exhibits a pattern of non-compliance, we take decisive action. This may include re-evaluation of our relationship, implementation of corrective measures, or, if necessary, termination of the partnership to protect our network and customers.

Through these "Know Your Upstream Provider" procedures, SIPSTACK ensures that our network is supported by partners who share our commitment to combating illegal robocalls and upholding the highest standards of telecommunications service. This proactive approach is a key component of our comprehensive strategy to provide a secure and trustworthy communication environment.

Respectfully Submitted,

SIPSTACK Inc.

Robocall Mitigation Inquiries:
+1 (416) 477-4644 x 763
rmd@sipstack.com