

ROBOCALL MITIGATION PLAN

This Robocall Mitigation Plan (“RMP”) outlines: (1) the targeted and prudent measures that IronSIP LLC (“IronSIP”) has implemented to prevent the transmission or handling of unauthorized robocall traffic; (2) IronSIP’s pledge to promptly and comprehensively address all traceback inquiries from the Federal Communications Commission (“Commission”), law enforcement agencies, and the industry’s traceback consortium within a 24-hour timeframe; and (3) IronSIP’s dedication to collaborate with these entities in identifying and halting any illicit robocall activities leveraging our services for call transmission or processing.

ENTITY COVERED:

- **IronSIP LLC**
11201 N Tatum Blvd Ste 300, Phoenix, AZ 85028
Operating Company Number (OCN): **676K**

STIR/SHAKEN STATUS:

- IronSIP has completed full implementation of the STIR/SHAKEN Caller ID Authentication Framework across its network.
- IronSIP is an iconectiv Authorized Service Provider in good standing with the STI-PA.
- IronSIP has secured its current STIR/SHAKEN certificate through Peeringhub, an approved Certification Authority.

DESCRIPTION OF ROBOCALL MITIGATION PLAN

Purpose

IronSIP is a Voice Service Provider dedicated to stopping illegal calls from originating in its network. As certified in the Robocall Mitigation Database (“RMD”), IronSIP has fully implemented STIR/SHAKEN. IronSIP submits this document addressing its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls.

Roles in the Call Chain:

IronSIP is a diverse service provider that serves various customer needs. It acts as a Direct Service Provider for residential customers, business customers, and resellers, while functioning as a Non-Gateway Intermediate Provider for our wholesale clients.

Know Your Customer (“KYC”)

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a

telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with IronSIP in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

IronSIP's KYC program involves obtaining specific subscriber information when the customer establishes service. This process includes collecting information such as:

- physical business location(s) or residential address;
- contact person(s);
- nature of customer's business

For resellers and Enterprise / Wholesale customers we also take the following steps:

- verify company info with relevant Secretary of State / Corporate Commission
- validate physical business address provided
- verify that the website for the company is valid and matches the business profile
- validate if a company has any social media presence
- perform various searches for any FCC/FTC/State AG complaints or actions

In addition, for Wholesale customers we employ additional steps:

- validate the company is listed in the RMD and the information matches the business profile provided by the company as part of our KYC questionnaire
- validate the company has an active FCC 499 registration which matches the business profile provided
- validate the company's STIR/SHAKEN compliance as specified in its RMD record and perform technical interop review session with the company's team to ensure proper STIR/SHAKEN integration with IronSIP's systems
- validate the FRN, OCN, and other regulatory information provided

Know Your Upstream Providers

In accordance with the Commission's directive in Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59 (Rel. May 19, 2023) ¶¶ 49-51, IronSIP provides the following information concerning its upstream voice carriers.

IronSIP receives voice traffic from the following upstream providers:

- 1) thinQ Technologies, Inc. DBA Commio
5420 Wade Park Blvd
Suite 100
Raleigh NC 27607

- 2) Bandwidth Inc.
2230 Bandmate Way
Raleigh NC 27607
- 3) Telnyx, LLC
311 West Superior St
Suite 504
Chicago IL 60654
- 4) FracTel, LLC
122 4th Ave.
Suite 201
Indialantic FL 32903
- 5) Bulk Solutions, LLC
704 N. King Street
uite 500
Wilmington DE 19801
- 6) Bulk Solutions, LLC
704 N. King Street
uite 500
Wilmington DE 19801

According to the RMD, thinQ, Bandwidth, Telnyx, FracTel, and Bulk Solutions are fully STIR/SHAKEN compliant and, to the best of IronSIP's knowledge, information, and belief, thinQ, Bandwidth, Telnyx, FracTel, and Bulk Solutions have been, and will continue to, sign calls transmitted to IronSIP, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to IronSIP.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity refers to the originating telephone number included within call signaling protocols, utilized for the purpose of caller screening. This identifier is uniquely linked to a subscriber and serves to establish the outbound caller's identity. Subscribers are authorized to employ a TN as their caller identity under the condition that the TN is either directly administered by IronSIP or secured through IronSIP from one of its partner carriers for subscriber usage.

IronSIP predominantly oversees the TNs utilized by its subscribers, maintaining a comprehensive inventory system to track these numbers and manage their allocation.

Should a subscriber intend to use a TN as their caller identity that is not under IronSIP's direct oversight, a process of TN validation becomes requisite. In instances where a subscriber can furnish a legitimate letter of authorization, verifying their entitlement to use the specified TNs,

IronSIP will proceed to authenticate calls initiated with these TNs, ensuring compliance and securing caller identity integrity.

Efforts to Avoid Carrying or Processing Illegal Robocalls

IronSIP is dedicated to the fight against illegal robocalls, investing in technology and strategies to prevent their transmission through its network. Utilizing analytical systems, IronSIP identifies potential robocall activity by monitoring indicators such as call duration, Answer Seizure Ratio (ASR), call volume, and carrier or consumer reports. Our approach encompasses a comprehensive suite of practices aimed at reducing the prevalence of unwanted robocalls for our customers, including:

- **In-depth Carrier Analysis**
 - **Upstream Provider Scrutiny:** IronSIP thoroughly reviews the credentials of upstream providers, ensuring they are not listed in the Robocall Mitigation Database (RMD) and that their Robocall Mitigation Plans (RMPs) effectively monitor and mitigate illegal robocall traffic.
- **Advanced Robocall Mitigation Tactics**
 - **Proprietary Software:** Our in-house software monitors voice traffic in real-time, employing behavioral analytics and caller authentication to prevent illegal robocalls. This includes:
 - **Fraud Detection:** Leveraging automated systems for rapid identification and mitigation of robocalling, caller ID spoofing, and spam. Upon detecting suspicious patterns, alerts are sent to our Network Operations Center (NOC) for immediate action.
 - **Subscriber Alerts:** Warning subscribers of potential fraudulent calls through customer support notifications.
 - **Call Blocking:** Empowering users with tools to block suspicious calls, supported by both custom and industry-standard number validation databases.
 - **Business Number Registration:** Safeguarding legitimate business numbers from being wrongly blocked.
 - **Caller ID Services:** Implementing Caller ID name services with fraud mitigation, ensuring accurate caller information is maintained even for flagged calls.
 - **Customer and Payment Verification:** Halting services to customers identified with fraudulent patterns, including invalid credit card use.
- **Operational Vigilance**
 - Proactive monitoring and analysis of call and account activities against expected patterns, including immediate investigation of any irregularities.
 - Validating the authenticity of call origins and engaging with subscribers directly to confirm the legitimacy of their activities.

- **Strict Enforcement Policies**

- **Contractual Termination Rights:** IronSIP reserves the right to terminate services for customers in breach of the law or Telephone Consumer Protection Act violations. Furthermore, IronSIP responds to regulatory actions by ceasing traffic from entities marked by the Commission or the Federal Trade Commission (“FTC”) for non-compliance or identified as illegal robocallers.

IronSIP remains vigilant in its efforts to protect its network and customers from the impact of illegal robocalls through a blend of technological innovation, strategic partnerships, and strict compliance with legal and regulatory frameworks.

Traceback Requests

IronSIP follows Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, IronSIP devotes sufficient resources to provide prompt and complete resources to traceback requests

IronSIP commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.

Customer Education

IronSIP posts information on its customer accessible sites to educate customers on how to protect themselves from becoming a victim of unlawful robocallers and a process to report complaints related to robocall activity. Customers are provided with self-serve portals and tools that enable them to block spam calls and/or individual numbers.

Commitment to Cooperate in Investigating and Stopping Illegal Robocallers

IronSIP also promptly responds to inquiries from law enforcement and regulators, including the Commission, FTC or state attorneys general seeking traceback or similar information. IronSIP commits to continue to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use IronSIP’s services to carry or process calls

Certifications

- IronSIP has not been prohibited from filing in the RMD due to an enforcement action.
- IronSIP is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. IronSIP will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, IronSIP will republish it to employees, consultants and contractors and file such an update to the RMD within ten (10) days of such update.

Aviv Shaham
President
IronSIP LLC

April 2, 2024