



**Sigma Broadband Co.<sup>®</sup>**

**ADDRESS**

2690 Cobb Parkway Suite A5-284 Smyrna, GA 30080

**PHONE**

(706) 744-6222 (706) SIGMABB

**ABOUT SIGMABROADBAND**

Sigma Broadband Co. is a growing company with a historic focus in the nurturing of business ideas demonstrating a positive upside, while striving to bring new technologies and unique products to their respective markets. With extensive holdings in the Global Telecom, Broadband Wireless, and IPTV sectors, Sigma Broadband delivers next-generation digital products to customers everywhere.

**WHO WE ARE**

Our multicultural leaders have deep start-up and enterprise experience, with rich mobile Broadband expertise.

**WHAT WE DO**

When we're not developing our own products and services, we continue to explore mergers and acquisitions with companies and other businesses.

This submission comprises the Robocall Mitigation Plan outlined by Sigma Broadband, proceeding in line with the norms of 47 C.F.R. § 64.6305. Sigma Broadband, as a voice

service provider prioritizes the implementation of robust strategies and measures with an aim to drastically curtail the propagation of illegal robocalls from within our network.

The following section presents our robust and meticulously crafted policies and systems that Sigma Broadband utilizes to deter and contain the repercussions of outbound illegal robocalls:

1. **Call Authentication:** Sigma Broadband employs state-of-the-art call authentication technologies, including but not limited to, the SHAKEN/STIR framework. This ensures the verification of calls from our network and curbs Caller ID spoofing, a tactic universally used by illegal robocallers.
2. **Call Monitoring and Analysis:** Sigma Broadband firmly believes in actively and continuously examining and scrutinizing call traffic by leveraging avant-garde analytics tools and algorithms. This aids us in discerning patterns and irregularities associated with robocalls and hence, take swift and necessary actions.
3. **Traffic Filtering and Blocking:** Sigma Broadband diligently puts into action traffic filtering and blocking mechanisms to thwart the generation of illegal robocalls proactively. These mechanisms are persistently updated based on industry gold standards and insights from our network monitoring initiatives.

Further steps, including customer education and awareness, cooperation and collaboration, augment our efforts in combating robocalls.

Sigma Broadband is fully cognizant of the adverse effects of illegal robocalls on the telecommunications industry. Our commitment lies in offering a secure voice service environment. We remain steadfast in our effort to take all plausible steps to prevent the generation of illegal robocalls on our network.

## **1. ADOPTION OF STIR-SHAKEN**

Sigma Broadband's status concerning the execution of STIR-SHAKEN, as recorded in the FCC's Robocall Mitigation Database, affirms that we have wholly embedded the STIR-SHAKEN authentication structure within our network. Calls made from our network are fully aligned with the guidelines of 47 CFR § 64.6301(a)(1) and (2). Also, our Robocall Mitigation Plan clearly outlines our strategies and regulations aimed at minimizing the chance of our service being utilized for illegal robocalls.

## **2. COMPLIANCE WITH TRACEBACK REQUESTS**

Our commitment to cooperate with entities such as the FCC, law enforcement, and ITG in our shared mission to discourage illegal robocall operations is solid. We ensure that all traceback requests and investigations received are responded to promptly. By assigning adequate resources, we aim to complete and provide responses to traceback requests ideally within a 24-hour period from receipt.

### **3. UTILIZATION OF ADDITIONAL SAFEGUARDS**

To enhance the trace back of any illegal robocalls put forth, we are careful to embed specific terms in our agreements with carrier interconnections and/or service providers. These contractual terms compel all parties to participate in the traceback process for voice service calls, whether it is identifying the upstream provider that allowed a suspected illegal robocall into their network or the customer who initiated the call. This measure strengthens the spirit of accountability and collaborative efforts in our fight against illegal robocalling activities.

### **4. REFINEMENT OF SUBSCRIBER VETTING MECHANISMS**

Sigma Broadband is dedicated to proactive measures that deter the rise of illegal robocalls, which includes an intense focus on refining subscriber vetting. By following industry-best practices, the identity of all our voice service subscribers can be confirmed. Thus, we cement the authenticity and credibility of customers, forming the foundation for a secure business partnership.

In a bid to adhere to legal norms and uphold ethical standards, Sigma Broadband uses a thorough vetting procedure. This scrutiny encompasses the stages of customer service requests, agreements, and assignment of phone number resources. Information such as a customer's physical location, primary contacts, incorporation details, federal tax ID and business nature are collected during the vetting process. This data collection not only helps to authenticate a customer's identity but it also provides us a means to gauge their suitability for the chosen services.

With respect to commercial end-users, especially bigger organizations with complex service configurations, Sigma Broadband recognizes the increased likelihood of their potential involvement in robocalling activities. Therefore, we may subject these customers to additional assessment, including stringent background checks and, potentially, on-site visits. These extra measures aim to ensure responsible use of Sigma Broadband's voice services by confirming the legitimacy of these customers.

We also apply a special scrutinization process for our wholesale customers. As part of our procedure, we may cross-verify their identity against the FCC Form 499-A Filer database or the FCC's Intermediate Provider Registry. If a customer is not registered

within these databases, additional investigation is conducted to understand the nature of the customer's business.

In regard to service agreements and acceptable use policies, Sigma Broadband promulgates strict guidelines to prevent both existing and new customers from engaging in illegal calling activities. These guidelines aim to stop any misuse of our services that could lead to violations of federal, state, or local laws, including involvement in fraudulent or deceitful activities. Our agreements explicitly instruct our customers that our services are not to be used to make illegal robocalls. We retain the right, communicated in our service agreements, to suspend or discontinue a subscriber's voice service if they violate any relevant service usage terms.

- Sigma Broadband has established a systematic process for continuous surveillance of network facility usage and performance. We routinely scrutinize our call detail records (CDRs) to detect any abnormal or suspicious calling patterns or activities that may imply the network is being used for initiating illegal robocalls. Upon detecting such activities that align with illegal robocall patterns, we reach out to the customer within a 24-hour window for a comprehensive investigation and possible redirection of their voice service.

## **I. VERIFICATION OF TELEPHONE NUMBER**

Our approach to number validation involves confirming the legitimacy of a customer or end-user's usage of a specific telephone number with their subscribed voice service(s). Aligning with industry best practices, Sigma Broadband implements measures to verify the user's right to utilize a telephone number. A user is permitted to use a number as their caller identity if it is controlled directly by Sigma Broadband or acquired through an underlying partner.

Moreover, for single-line voice service users, our switch equipment is configured to accept calls only from the number assigned to that user. For users with multi-line telephone systems, Sigma Broadband screens all outgoing calls, allowing connection only if the origin number corresponds to one of the numbers allocated to the subscriber. This automatic validation method ensures the security and validation of originating phone numbers.

## **II. ORIGINATORS OF INTERNATIONAL CALLS**

Sigma Broadband currently does not provide international voice services and has no plans to extend such offerings.

### **III. KNOW YOUR CUSTOMER**

1. Our Sales, Product Management, and Business Operations teams conduct a potential risk analysis, which includes an evaluation of the customer's intended traffic type, types of end-users served, and the principal locations the customer plans to make calls to.
2. We require customers to furnish their official business name, business address, contact details, and tax or other official ID; this information is reviewed by our Finance team. They undertake a search engine investigation to verify the carrier's authenticity and also evaluate the carrier's financial stability.
3. Included in our customer contract is the requirement for customers to actively work towards eliminating fraud and misuse related to the traffic forwarded to Sigma Broadband. They are also instructed to cooperate on all issues concerning fraudulent traffic.
4. Sigma Broadband employs a combination of automatic systems and manual intervention for assessing the legitimacy of all incoming voice interactions. This includes the use of analytical tools and specific call handling techniques.

In conclusion, Sigma Broadband upholds the Know Your Upstream Provider (KYC) approach by exerting thorough due diligence with our direct upstream customers.

### **VII. SUSTAINED ROBOCALL MITIGATION EFFORTS**

Sigma Broadband diligently observes its network usage and ritually assesses call detail records (CDRs) with the intent to discern any irregular call activities or patterns. Whenever network usage patterns pointing towards illegal robocalls are noticed, or Sigma Broadband suspects illegal robocalling or spoofing activities on its network, immediate steps are taken to identify the party engaged in such practices. Identified parties may then be subjected to appropriate actions, which may include initiating traceback investigations, verifying the ownership or authorized usage of the Caller ID number by the originating customer, ensuring the Caller ID name dispatched to a receiving party aligns with the customer's trademark, registered name or d/b/a name, discontinuing the party's ability to initiate, terminate, or route calls on Sigma Broadband's network, and notifying law enforcement agencies.

As a commitment to prevent and mitigate the origin of robocalls in its network, Sigma Broadband centers its focus on early identification and thorough investigation of possible robocalling activities. In monitoring its network usage, certain red flags that are

specifically noted include; (1) unusual subscriber traffic volume, large traffic bursts within short periods, or irregular traffic volumes (usage spikes), (2) initiation of short duration calls and low call completion percentages, (3) Outgoing calls with sequential dialing patterns, (4) Multiple calls made to numbers listed in the do-not-call registry or invalid numbers, and (5) Calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

### **VIII THIRD-PARTY CALL ANALYTICS**

Sigma Broadband employs third-party call analytics to aid in preventing the origin of illegal robocalls within its network. Detailed in **Appendix A** are the names of the vendor(s) deployed, alongside a rundown of the call analytics system(s) used to detect and block illegal robocall traffic.

#### **Call Analytics Vendor Information and System Description:**

Vendor Name: Internal Proprietary Tech

System Overview: The call analytics system procured from the vendor scrutinizes if outgoing calls should be blocked. If the telephone number is either listed in a Do-not-call registry or is otherwise an unoccupied, underused, or invalid number, the call is deemed to be fraudulent and is marked as a requirement for blocking. The vendor may further employ advanced fraud detection which empowers behavior analysis and tracking of abnormal or unanticipated calling patterns to detect high volume robocalling, spoofing, and suspicious call activities.