

CHARGER ACCESS, LLC.

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Charger Access (“Charger” “the Company”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This document describes the status of its implementation of STIR/SHAKEN and the practices and procedures Charger has in place to mitigate illegal robocalls. Charger may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

Charger has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, and none of its prior certifications have been removed from the Database by the Commission.

Charger has not been, at any time in the prior two years, the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with Charger’s findings of actual or suspected wrongdoing due to it transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Charger Access primary place of business is:

206 Gothic Ct.; Suite 304
Franklin, Tennessee 37067
615-656-8151
General email address: info@chargeraccess.com
Website: www.chargeraccess.com

Leaders of the Charger Access are:

CEO:

Rusty Hagenbuch
206 Gothic Ct.; Suite 304
Franklin, Tennessee 37067
Phone: 615-224-8422
Email: rusty@chargeraccess.com

CTO:

Name: Michael Hyams
206 Gothic Ct.; Suite 304
Franklin, Tennessee 37067
Direct Dial: 615-622-4603
Email Address: michael@chargeraccess.com

Designated RMD Contact:

Rusty Hagenbuch
206 Gothic Ct.; Suite 304
Franklin, Tennessee 37067
Phone: 615-224-8422
Email: rusty@chargeraccess.com

STIR/SHAKEN IMPLEMENTATION

Charger is in full compliance with all conditions set forth in the FCC’S 2020 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission’s rules and policies more generally.

Charger Has implemented STIR/SHAKEN through use of multiple TransNexus products (Call Guardian and others) in conjunction with using the Charger IPES OCN code. This is a managed end-to-end call authentication solution that fully satisfies the FCC’s STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226 and SHAKEN – ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

Charger has deployed call authentication, call labeling, and call blocking services provided by Transnexus, and iConectiv and has made great strides to, at all times protect the Company’s network and customers from harmful calls. Though the use of TransNexus Call Blocking Services Charger supports comprehensive call blocking services that include Do-Not-Originate (DNO) detection, reporting, and blocking across the Company’s network. These services are designed to protect consumers from unwanted and illegal calls, particularly robocalls.

The DNO list that Charger uses is maintained by TransNexus and entities like them and is used by the Company to identify, report on, and block calls that transit through the Charger network. To ensure that Charger has implemented a complete solution to its full network so that all customer calls are fully attested and authenticated.

ROBOCALL MITIGATION PLAN

This Robocall Mitigation Plan describes the specific measures that the Charger has implemented to detect and prevent illegal robocalls on its network. Charger will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should the Charger determine that changes are appropriate, its practices may differ from those described below.

Risk Assessment. Charger is a voice service provider offering a variety of voice calling services. Its customers generally do not originate High Volume Short Duration (“HVSD”) calling patterns and Charger has not received information suggesting that robocalls originate on its network. Therefore, Charger does not consider its network at high risk of originating illegal robocalls.

Additionally, as mentioned throughout this document Charger leadership takes additional steps to always ensure that the Company's network is not only at the highest level of STIR/SHAKEN and Robocall Mitigation compliance. The Company is constantly monitoring its network in order to fully comply with the FCC Orders and mitigate and minimize risk.

KNOW YOUR CUSTOMER

Charger has a rigorous KYC policy for the in order to support the Business Customers that it resells services to. Charger has an in-depth presales process where representatives of work with the prospect or customer to understand all the unique factors of the Customer's business. The objective of this is two fold: a. to get to know the customer; and b. to provide the best possible service to the customer by fully understanding all facets of their business.

Charger performs a thorough reputation check on each of its customers and verifies the following information: legal business name, legal form of business, federal tax ID, nature of the business, primary contact person, and service address.

Not only does Charger have a rigorous intake and Onboarding process where it secures extensive information for Customers but all relationships between Charger and customers are governed by an MSA. The MSA specifically states the business customer is not able to resell any services are sold to the customer by Charger.

The Company performs a thorough credit check on each of its customers and verifies the following information: legal business name, legal form of business, federal tax ID, nature of the business, primary contact person, and service address.

Charger conducts due diligence on new and renewing customers, confirming the customer's identity and, if it is a business, is incorporation documents. Charger confirms the customer's service address for all customers.

- Charger verifies customer's business reputation prior to providing service.
- Charger verifies customer information when contracts are renewed or services are added.
- Charger verifies the customer's identity and their right to use the telephone number presented on calls.
- Charger has a specific Acceptable Use Policy ("AUP") which defines all Company the policies regarding the circumstances by which Charger will deny, suspend or terminate service to a customer.

When the Company commences operations with a customer, the Company verifies all new customers with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and

employees. The Company severely limits the capabilities of new accounts until these appropriate processes are complete.

Additionally, as mentioned above, all Company customers are required to agree to, and; are contractually bound by Charger strict policies, contractual terms and conditions and a Company Acceptable Use Policy (“AUP”) prohibiting the act of fraudulent voice activity as a condition of doing business with Charger.

If any customer is found to be in possible and/or or actual violation of any Company policy as it relates to suspicious traffic and/or possible fraud, the Company has the right to immediately halt, cease and/or suspend the customer’s account or associated telephone numbers and block all calls and usage.

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

(Current & Ongoing)

The Company always employs real-time controls on traffic. All calls have valid caller-ID values and ANI. Each customer has a calls-per-second limit commensurate with the traffic description provided and stated in the Customer Agreement and Service Order; as applicable.

Charger certifies that it will cooperate with such entities in investigating and stopping any illegal robo-callers that use its service to originate calls, Charger also certifies that all voice traffic which originates on its network is subject to the Company’s robocall mitigation program.

Charger multiple analytics technologies and services (like TransNexus) to monitor traffic on its network and identify potentially unlawful call origination activity. If Charger has a reasonable basis to believe that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, Charger can suspend and/or terminate service to the customer as defined further in this document.

Along with full network monitoring, the Charger team has a fully deployed call record monitoring program which allows the Company to process Call Detail Records (“CDR”s) by exporting the data from the Charger switch. These CDR’s can be used at any time to help identify potential illegal robocalls. The CDR’s are analyzed and summarized to immediately recognize traffic that has the characteristics of illegal robocall traffic.

As mentioned above under the risk assessment this monitoring includes High Volume, Short Duration (“HVSD”), sequential dialing patterns, calls to NPA-NXXs that may not be assigned by the North American Numbering Plan Administrator and other best practices Charger leadership has identified relative to the to combat identifying illegal robocalls.

Additionally the Company has designed, developed and deployed monitoring, diagnostics and analytical tools in conjunction with third party application as part of the Company’s network infrastructure and switching protocols. These analytical and diagnostic tools provide detailed call traces for the Company to review, monitor, diagnose and collect data associated with calls traversing the network.

When investigating suspicious traffic, the Charger network and technical teams use tools and analytics which are database driven to search for traces on particular lines or Customers and to view the traces. The tools which the Company employs also allow traces to be printed or exported for offline storage for further evaluation if required. The traces include decoded signaling messages, routing and number validation events, call service actions/decisions, codec selection, echo cancellation programming, media events such as digit and tone detection, tone generation, and digit out-pulsing, billing records and concise call logs. This collection of data allows for a comprehensive ability to monitor network traffic.

This monitoring is conducted in accordance with the Company's best practices (at least 3 times weekly) and also, of course as soon as the Charger team becomes aware of any suspected nefarious calling activity by a customer. Additionally the tools which the Company has deployed do have alerts and alarms which sound if and when suspicious calling patterns are present along with numbers that are not recognized.

If the Company's monitoring process identifies the potential of illegal robocalls originating from the network, the Company will follow the internal policy and procedure and shall immediately halt, cease, suspend or terminate the Customer and of course the offending numbers and associated calling traffic.

RESPONDING TO TRACEBACK REQUESTS

Charger has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. Upon receipt of the first request from the ITG The Company will inform the ITG staff of the proper Robocall Mitigation Database Contact for Charger (if it has not done so already). Additionally Charger complies with all the requirements, regulations and guidelines as set forth by the ITG as noted <https://www.ustelecom.org/the-industry-traffic-group-itg/for-providers/>

Charger will respond within 24 hours of receipt of traceback request to inquiries received from the Industry Traceback Group. If a pattern of questionable activity is detected, Charger will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Charger is committed to respond within 24 hours to any and all requests from CALEA, the Industry Traceback Consortium, and all law enforcement agencies who officially and properly subpoena customer records.

Charger is committed to cooperating with the Federal Communications Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robo-callers that it learns are using our service to originate calls or transit calls into the United States and territories.

The Company commits to fully responding within 24 hours to all traceback requests from the ITG, the TPTG, the FCC, and law enforcement. The Company shall cooperate with these

groups to investigate and stop any illegal robo-callers from using the Company's service to carry or process illegal calls.

When notified by the FCC's Enforcement Bureau, Company shall block and report identified illegal traffic, and any substantially similar traffic, on an ongoing basis when Company receives actual written notice of such traffic from the Enforcement Bureau. The Company shall provide the Enforcement Bureau with an explanation as to why Company reasonably concluded that the identified traffic is not illegal, and what steps it took to reach that conclusion.

As mentioned in other sections of this document, the Company utilizes a combination of tools provided by its underlying carriers and platform providers along with third-party solutions to check for Do Not Originate (DNO) numbers. In addition, the Company utilizes a combination of internal tools and third-party solutions to detect invalid phone number formats, area codes and unassigned number blocks. The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

UPSTREAM PROVIDERS

The Company only uses upstream providers that are listed in the RMD and maintains a robust fraud detection system. In addition, any upstream provider must possess the ability to connect, in real time, with the Company so that issues with calls being processed by the Company can be immediately identified and addressed.

Two of the Company's upstream providers are:

1. VoIP Innovations
8 Penn Center West Suite 101
Pittsburgh, PA 15276
General Phone Number: 877-478-6471
Website Address: www.sangoma.com
General Email: support@voipinnovations.com
2. Bandwidth (aka Bandwidth CLEC)
900 Main Campus Dr,
Raleigh, NC 27606
General Phone Number: 855-864-7776.
Website Address: www.bandwidth.com
General Email: support@bandwidth.com

COMPANY DECLARATION

The Company certifies that it has never been under investigation or committed any violations within the last two years with any local, state, or Federal agency or equivalent related to telemarketing or robocalling. Additionally, the Company is not currently subject to formal action or investigation due to suspected unlawful robocalling or spoofing. If when and as the Company business may change designated Company representatives only will update this RMP as appropriate.