

Robocall Mitigation Plan

This Robocall Mitigation Plan is being submitted by [Provider Name], in accordance with the requirements of 47 C.F.R. § 64.6305. As a voice service provider, we are committed to establishing and implementing effective measures to reduce the occurrence of illegal robocalls originating on our network.

Outlined below are the policies and procedures that Flash Telecom Systems, LLC currently has in place to mitigate the impact of outbound illegal robocalls:

1. **Call Authentication:** We have implemented call authentication technologies, such as the SHAKEN/STIR framework, to verify the legitimacy of calls originating on our network. This helps prevent the spoofing of Caller ID information, a common tactic used by illegal robocallers.
2. **Call Monitoring and Analysis:** We actively monitor and analyze call traffic on our network using advanced analytics tools and algorithms. This enables us to identify patterns and anomalies associated with robocalls, allowing us to take prompt and appropriate actions.
3. **Traffic Filtering and Blocking:** To proactively prevent the origination of illegal robocalls, we employ traffic filtering and blocking mechanisms. These mechanisms are continuously updated based on industry best practices and intelligence gathered from our network monitoring activities.
4. **Customer Education and Awareness:** We are committed to educating our customers about the dangers and impact of robocalls. Through various communication channels, we provide information and resources to help our customers understand how to protect themselves from illegal robocalls and how to report any suspicious activity.
5. **Cooperation and Collaboration:** Flash is dedicated to collaborating with industry stakeholders, including the FCC, law enforcement agencies, and industry groups like the ITG. We commit to promptly respond to traceback requests within 24 hours, and to actively cooperate in any investigations aimed at identifying and stopping illegal robocallers using our services. By implementing these policies and procedures, we demonstrate our commitment to combatting the issue of illegal robocalls and protecting against unwanted and fraudulent calls. We continuously assess and update our strategies to stay ahead of evolving robocall techniques and ensure the effectiveness of our mitigation efforts. We h

Flash is fully aware of the negative impact of illegal robocalls and the telecommunications industry. We remain dedicated to providing a safe and secure voice service environment, and we are committed to taking all reasonable steps to prevent the origination of illegal robocalls on our network.

I. STIR-SHAKEN IMPLEMENTATION STATUS

The Provider's status regarding the implementation of STIR-SHAKEN is as follows, according to the FCC's Robocall Mitigation Database:

Flash Telecom Systems, LLC has successfully implemented the STIR-SHAKEN authentication framework on its network. Calls originating from our network are compliant with the regulations stated in 47 CFR § 64.6301(a)(1) and (2). The Provider has also established policies and procedures outlined in its Robocall Mitigation Plan to prevent the use of its service for illegal robocalls.

II. TRACEBACK REQUESTS

The Provider acknowledges its commitment to support and collaborate with the FCC, law enforcement agencies, and the (ITG) in tackling illegal robocall activities. This includes promptly responding to and complying with all traceback requests and investigations. The Provider will allocate adequate resources to ensure the completion and provision of responses to traceback requests within a reasonable time frame. It commits to responding fully to any traceback request received within 24 hours of receiving the request.

III. ADDITIONAL MEASURES

As a measure to facilitate the effective traceback of illegal robocalls, the Provider will now incorporate specific provisions in its carrier interconnection and/or service agreements. These contractual clauses will require all parties involved to cooperate in the traceback process of voice service calls. The provisions will outline the importance of promptly identifying the upstream provider responsible for introducing a suspected illegal robocall into their network or the customer from whom the call originated. This step will enhance collaboration and accountability among parties in combating illegal robocalling activities.

IV. CUSTOMER VETTING PRACTICES

As a measure to prevent or minimize the occurrence of illegal robocalls originating from its voice services, the Provider will implement industry best practices to verify the identity of all its voice service subscribers. The subscriber vetting process aims to ascertain the authenticity and legitimacy of customers, forming the basis for establishing a business relationship.

To ensure compliance with legal requirements and promote ethical conduct, the Provider implements a comprehensive vetting process. This process takes place during the provisioning of customer-requested services, execution of service agreements, and allocation of telephone number resources. During the vetting process, the Provider collects essential information from customers, such as their physical location, contact person(s), state or country of incorporation, federal tax ID, and details regarding the nature of their business. Gathering this information helps confirm the identity of customers and assess their suitability for the services they seek.

For commercial end users, particularly larger businesses with more intricate service configurations, the Provider acknowledges the increased risk of potential involvement in illegal robocalling activities. Accordingly, the Provider reserves the right to subject such customers to additional scrutiny, which may involve more stringent background checks and, in some cases, site visits. These additional measures aim to further ensure the legitimacy and responsible usage of the Provider's voice services. The Provider also understands the special importance of vetting any wholesale customers it may have. If necessary, the Provider may vet identity information for its wholesale customers by confirming whether the customer is an FCC Form 499-A filer in the FCC Form 499-A Filer database or in the FCC's Intermediate Provider Registry. If the customer is not registered within those databases further investigation is conducted to better understand the nature of the customer's business.

Additionally, the Provider implements service agreements and acceptable use policies to ensure that both new and existing customers refrain from making illegal calls. These agreements and policies are designed to prevent the misuse of voice and broadband services in a manner that violates local, state, or federal laws, including engaging in deceptive or fraudulent activities. The documents governing the use of Provider-provided services explicitly state to all customers that their services must not be used for illegal robocalls. Furthermore, the Provider retains the right, as stated in its service agreements, to suspend or terminate a subscriber's voice service if they violate any relevant terms related to service usage.

- Has established a routine process for monitoring of the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where the Provider identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within 24 hours for further investigation and possible action regarding their subscribed to voice service.

V. TELEPHONE NUMBER VALIDATION

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner. Further, for: (1) single line voice service subscribers, both services connected via TDM or IP, the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, for both services connected via TDM or IP, the Provider screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

VI. INTERNATIONAL CALL ORIGINATORS

Flash is not currently an international voice services provider and has no plan to offer services.

VII. KNOW YOUR CUSTOMER

1. Sales, Product Management, and Business Operations teams conduct risk assessments. This involves evaluating the type of traffic the customer intends to send and the type of end users served by the customer. The primary locations to which the customer will send traffic are also reviewed.
2. Customers are required to provide their legal business name, business address, contact information, and tax or other regulatory ID. This information is reviewed by the Finance team, which also conducts a search engine investigation into the legitimacy of the carrier in question and evaluates their financials.
3. Contract language mandates that customers agree to work towards eliminating fraud and misuse related to the traffic sent to Flash. They are also required to cooperate on all issues relating to fraudulent traffic.

4. Flash uses a combination of automatic systems and manual resource efforts for evaluating the legitimacy of incoming voice communications. This includes utilizing analytics and call handling techniques.

In summary, Flash takes the Know Your Upstream Provider (KYC) approach seriously by conducting due diligence on their immediate upstream customers.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on the Provider's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to 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

The Provider also uses third-party call analytics to further assist and prevent the origination of illegal robocalls on its network. Included in **Appendix A** is the name of the vendor(s) used along with a description of the call analytics system(s) used to identify and block illegal robocall traffic.

Call Analytics Vendor Name and Description of System:

Name of Vendor: TransNexus

Description of the call analytics system Call analytics purchased from the vendor determine if originating calls should be blocked. If the telephone number appears on a Do-not-call list or otherwise is an unallocated, unused, or invalid number, the call will be determined to be fraudulent and needs to be blocked. Vendor may also use advanced fraud detection which enables behavior analysis and tracking of abnormal and unexpected calling patterns to detect high volume robocalling, spoofing, and suspicious call activity.