

SoftWave Telecom LLC ROBOCALL MITIGATION PLAN

Below is the Robocall Mitigation Plan filing for SoftWave Telecom LLC This plan will be submitted to the FCC's Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices.

SoftWave Telecom LLC has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of nonvalidated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

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

SoftWave Telecom LLC accepts pre tokenized calls. No unsigned calls will be able to go over our network. We do sign our retail clients calls with a A attestation. Furthermore, SoftWave Telecom LLC is a Voice Service provider for our retail traffic only. We attest all retail traffic that is being dialed through our network with a A attestation if they use our DIDs, and since we manage their campaigns and know what traffic they are sending. We make sure they are on our platforms otherwise we dont sign random clients traffic at all. They are identified by their company name and filled out our kyc. We dont sign any traffic coming from outside our software. All traffic that we sign are from our software only others that are sending us traffic we make sure they sign their own traffic. We also monitor the traffic in our software by Sip Shield (SS) from Telucom LLC on our software that monitors in real time messages that are being uploaded into our software or monitors calls that are being made in real time as well. If we catch anything with (SS) the account gets locked down and wont get activated again until one of two people on management checks the violation and either let them back on or terminate immediately. 1 violation of uploading scam or fraud traffic is immediately blocked forever. No second chances. No wholesale client will send a C attestation traffic all will be A or B attestation. No C level attestation traffic at all will be accepted. And all unsigned calls will not be permitted on our network.

Softwave Telecom LLC has retail traffic on their routes. We make sure they fill out a kyc form with their company name and contact details and we also make sure they are either using optedin traffic or we will turn on dnc filter for their traffic. If they are using optedin traffic we make sure that we verify the optedin leads and make sure that they are opt ins with clients name and IP address and address to the client. We verify their landing pages and read their privacy policies and terms & conditions and AUP on their website and make sure they have compliant with TCPA and optedin jargon on their landing pages. Then we spot ck the clients at random when they are dialing we ask them for random optedin information so that at the chance they take longer than an hour we turn on dnc and don't turn it off till we get the optedin information for that client that we requested. Our attorney Patrick Crocker also cks his database for any infractions from the fcc or ftc or tpc violations in the past for the client that is using our software. If they fail at this stage we don't on board them. Even if the client had a previous company and they got in trouble its not worth the risk for us.

SoftWave Telecom LLC is judiciously working to prevent unlawful robocalls from originating on its network while we have implemented the new STIR/SHAKEN authentication architecture. SoftWave Telecom LLC ensures rigorous compliance with the STIR/SHAKEN standards and the Pallone Thune Telecom Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. The Company has implemented the following robocall mitigation plan to address unlawful robocall traffic.

SoftWave Telecom LLC also implemented Voice Shield and Roboguard through fraudcentral.io, SipShield through Telucom LLC and Smart Shield through Veriswitch to monitor our traffic. We also have implemented valid anion all of our traffic to prevent any spoofing.

SoftWave Telecom LLC also validates that the entity has a legitimate right to use its asserted calling numbers by activating and validate to all calls.

SoftWave Telecom LLC contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service.

Soft Wave Telecom LLC requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.

Prior to installing services for new customers, SoftWave Telecom LLC takes the following measures to weed out end users that could potentially generate robocall traffic: Our Know-Your-Customer (K YC) confirms the following about its customers:

Customer's identity
Service Address
Customer's right to use the telephone number
presented on calls
Authenticated legal campaigns and compliance
499 Filer ID
Robocall Mitigation Plan and RMD #
FEIN Number Customers Tokens

SoftWave Telecom LLC's contract explicitly prohibits the initiation of illegal robocalls, with immediate termination for non-compliance.

When the customer is a business, SoftWave Telecom LLC requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

SoftWave Telecom LLC will immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If the Company determines that the traffic was likely unlawful, then we terminate without prejudice.

SoftWave Telecom LLC will comply fully with all conditions set forth in the FCC'S 2024 Report and Order Mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

SoftWave Telecom LLC has designated an individual as a dedicated point of contact for addressing traceback requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. SoftWave Telecom LLC will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.

If SoftWave Telecom LLC detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. And terminate immediately. We are first and foremost a software company so we have all the bells and whistles to prevent unlawful robocalls or scam and fraud traffic from getting into America.

Appropriate action will

- Terminate client

SoftWave Telecom LLC will provide valid law enforcement and regulatory agencies with the relevant nonproprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated Robocall Mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. We respond within 24 hours to all traceback requests from the Commission, law Enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use the Company's service to originate, carry, or process illegal robocalls.

Soft Wave Telecom LLC performs the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. SoftWave Telecom LLC has not had any agency action or investigation due to suspected unlawful robocalling or investigations.

SoftWave Telecom LLC follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers.

This process includes a KYC and the collection and review of entity-identifying information to confirm that Soft Wave Telecom LLC has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.