

Saltech Systems is a VoIP provider offering hosted PBX and SIP trunking to small and medium sized businesses. Our customers are exclusively business end-users; we do not offer services to other telephone service providers or individuals. Our customers interconnect with us over the public internet using their own broadband service.

To combat the abuses of robocalling, Saltech Systems is actively working to implement a robust call authentication framework, while also working diligently to stop illegal number spoofing. We work directly with our end users so there is no authorized use of our systems.

Know Your Customer:

Each Saltech Systems customer must provide a physical business address, business registration, and name and contact information for at least one responsible individual. The business must have a web presence and contact email must be a domain dedicated to the business. The business must be registered in a US state or territory. Payment must be via credit card or US bank transfer. We cross-check and verify all these items and refuse to serve customers that are in any way suspicious. We do not serve foreign customers.

We have adopted a three-pronged operational approach (prevent, detect, and mitigate) to stop and prevent illegal robocalls, while also expanding on industry efforts and best practices, as well as aligning with the Federal Communications Commission's (FCC) guidance:

Here's the summary of our operational procedures to stop and prevent illegal robocalls:

Prevention:

Saltech Systems is working vigorously to prevent unlawful robocalls originating from our network. We rely on technologies from Bandwidth, our SIP Trunk provider to also block robocalls at the transport layer. We have implemented a stringent screening process that prevent companies with potentially fraudulent robocalling traffic from becoming Saltech Systems customers. We have also informed and empowered our customers with the information necessary to identify these unlawful calls, as defined by the FCC.

Detection:

Saltech Systems has automated systems dedicated to identifying and analyzing potential robocall campaigns on our infrastructure, and determining if they are lawful or not. In alignment with the FCC rules, our partner and vendor (Bandwidth) is in the midst of augmenting its robocall detection technology that identifies and blocks unlawful robocalls from traversing their network.

Mitigation:

Once an unlawful robocall campaign is detected, Saltech Systems takes several steps to stop all current and future unlawful calls. We have developed call blocking tools that prevent calls with specific unlawful ANI/'FROM' TN characteristics from traversing the Saltech Systems network. Saltech Systems personnel regularly analyzes network traffic looking for unlawful robocall campaigns and utilizes our call blocking

tools when appropriate. We work diligently with our customers to stop all detected unlawful robocall campaigns and proactively communicate with those customers that may be in the path of unlawful robocalls.

Saltech Systems uses several techniques. These include but are not limited to:

Blocklists: A blocklist is a database of phone numbers that are known to have originated spam calls. While this is not necessarily the "silver bullet" that some might hope it to be, it is an excellent start to prevent calls from these numbers from passing through your network.

Rate Limits: All callers are limited in the number of outbound calls they can initiate per minute and the number of concurrent calls allowed. These limits are set on a customer-by-customer basis based on conversational calling expectations given their business profile. A medium-sized business with 50 employees would be allowed 20 simultaneous calls and would be able to initiate 10 calls per minute.

Caller-ID: We provide our customers with their telephone numbers (DIDs); customers can port their numbers to Saltech Systems if they choose. All outbound calls must use a Caller-ID from that customer's pool of numbers assigned by us. The only exception is forwarded calls; in these cases, the call must include a DIVERSION header that contains a number assigned to that customer by Bandwidth. These conditions are checked by our switch before the call is sent onward.

CDR Monitoring: Saltech Systems assesses each customer's traffic on a weekly basis. We examine a set of metrics (number of call attempts, answer seizure ratio, average call duration, fraction of calls shorter than 60 seconds), looking for: (a) signs of automated dialing; (b) significant change from that customer's historic usage. Any anomalies result in immediate engagement with the customer to obtain a thorough, definitive explanation. If not resolved within 7 business days, the customer's service is suspended.

Traceback: Saltech Systems responds promptly to all traceback requests. Any traceback results in an immediate detailed analysis of the initiating customer's CDRs for the past 30 days, followed by engagement with the customer to explain anomalies in the CDRs as well as the specific traceback example. If we do not receive satisfactory explanation within 72 hours, the customer is suspended. A customer that is the subject of three tracebacks in 90 days is permanently banned from our platform, unless the traceback examples are shown with certainty to be legal and compliant.

Extension: Because we cannot get an SPC token today, Saltech Systems is subject to a STIR/SHAKEN implementation extension. Saltech Systems does not have direct access to numbering resources; we get our numbers via another wholesale provider (Bandwidth). We also have fewer than 100,000 customers.