

Smartcom Telephone, LLC
600 Ash Ave
McAllen, TX 78501

Robo-Call Mitigation Plan

This Robocall Mitigation Plan is submitted by Smartcom Telephone, LLC (“Provider”) pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all “voice service providers” to establish a “robocall mitigation plan”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR-SHAKEN IMPLEMENTATION STATUS

Smartcom Telephone, LLC (“Smartcom”) is eligible for the continuing extension of the STIR SHAKEN implementation deadline on Non-IP networks as a small voice service provider (§64.6304 (a)(2)) that has non-IP portions within its network §64.6304(d).

Smartcom provides local services to fewer than 100,000 voice subscriber lines. The majority of customers are served on the non-IP portions of Smartcom’s network which relies on technology that cannot initiate, maintain, carry, process, or terminate SIP Calls.

Consistent with §64.6303 (a)(1), Smartcom is working to upgrade its network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework. Smartcom’s non-IP network is connected to carriers that do not support IP connectivity. Therefore Smartcom can not yet fully upgrade its non-IP network to IP standards.

Smartcom’s network also has IP-portions which originate calls via SIP connections to other carriers. Smartcom has registered with the STI Policy Administrator under our OCN 4866, and is an authorized service provider in the STIR/SHAKEN ecosystem. Smartcom has implemented STIR/SHAKEN within the IP portions of its network and signs the calls originating on the IP portions of the network using our certificate.

As indicated in the FCC’s Robocall Mitigation Database, the Provider’s status with respect to STIR-SHAKEN implementation is as follows:

- Smartcom has not directly implemented the STIR/SHAKEN authentication framework on any portion of its network and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider’s service to originate illegal robocalls.

- Presently, the majority of voice traffic leaving Provider's Network utilizes "TDM" routing, which does not allow for any trust attestation to be incorporated. Provider performs its STIR/SHAKEN obligations through a partner carrier (ANI Networks) as this carrier handles 100% of the outbound SIP traffic originated. For calls originating from Smartcom, ANI Networks uses Smartcom's
- All IP Voice Traffic destined to Provider's network will come from either ANI Networks or Sinch (formerly Inteliquent).
- Provider is currently implementing new hardware which will allow enable us to move our secure token back to our own network and affix our own trust attestation without relying on third-party assistance. At that point we would be considered to be fully implemented.

II. TRACEBACK REQUESTS

As noted above, the Smartcom will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, Smartcom will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback request received within 24 hours after receiving the same.

As part of its efforts to assist in the successful traceback of illegal robocalls, Smartcom will going forward include within any new carrier interconnection and/or service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall entered its network or the customer of the service from which the call originated

III. CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, Smartcom will use best practices in vetting the identity of all of its voice service subscribers, whether a residential or business/commercial subscriber. The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, Smartcom looks to confirm the identify of customers using its voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Smartcom's efforts to vet retail and business/commercial subscribers occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing Smartcom's required service agreements, and granting the customer the right to use telephone number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers,

at the Smartcom's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, Smartcom:

- Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice and broadband services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of Smartcom's provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and Smartcom reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.
- 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 Smartcom identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within twenty-four hours for further investigation and possible action regarding their subscribed to voice service.

IV. TELEPHONE NUMBER VALIDATION PRACTICES

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, Smartcom has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of Smartcom's services is permitted to use a telephone number as their caller identity if a number is directly managed by Smartcom and/or obtained 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, Smartcom 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.

V. INTERNATIONAL CALL ORIGINATORS

Smartcom is not currently an international voice services provider

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a small provider of voice services, the number of upstream providers used by the Smartcom to receive and deliver its originated voice calls for termination are limited. Smartcom has

longstanding relationships with these upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, Smartcom, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking those steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any future contracts that Smartcom may directly have with any upstream provider entities.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

Smartcom 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 Smartcom 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 Smartcom's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, Smartcom is committed to early identification and investigation of possible robocalling situations. We are currently working with our billing/toll rating vendor to analyze and report anomalies in our call records to identify patterns such as:

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 ANALYTICS

As indicated in Section VI, Smartcom is currently working with our billing/toll rating software vendor (Communications Data Group) to enhance analytics of call traffic.

SUMMARY

Fortunately, Smartcom is a small-enough company that we have can maintain close relationships with the majority of our customers. This is especially true for those customers who have trunk groups (such as ISDN-PRI or SIP Trunking) that would allow any degree of mass calling and/or the ability to manipulate a customer-provided number on originating calls. The majority of our customers are State, County or Local Governmental entities, medical facilities and educational facilities from K-12 to State Universities.

Because of this, it is an easy task for Smartcom to trace any originating telephone number back to the source if there is a need for doing so, and the request for such traceback is done in a timely manner after the suspicious call was made. Smartcom will participate in any valid traceback investigation originated by the FCC, law-enforcement entity or the industry traceback consortium.

Other steps taken by Smartcom that will help mitigate RoboCalls or other malicious calling:

- 1) Through its billing vendor, receives weekly notifications of non-matching telephone numbers on calls originating calls through our network (numbers not found in our billing records).
 - a) Calls are scrutinized to find the source of the call.
 - b) These are occasionally a forwarded call that preserved the original caller's telephone number. However, if the reason for the use of an unidentified number cannot be determined, or if it appears to be a practice of advertising a non-Smartcom phone number as the originating TN, we open an internal case and our customers are contacted and given notification that this practice is not acceptable.
 - c) Often, the invalid number ends up being due to a misprovisioned station in the customer's network and corrections are made by the customer within a timely manner.
 - d) Once we know the matter has been resolved, the case is closed.
 - e) To-Date, we've had only a few cases in which the customer has refused to correct the calling number. In those cases, we blocked their ability to send such Customer Provided Numbers as the originating telephone number until such time as the matter was corrected.
- 2) Smartcom does not allow any traffic origination outside of company-owned networks. All traffic originates on facilities either owned or leased by Smartcom. No third-party traffic relay is allowed. Most of our SIP trunking customers are assigned private IP assignments that remain wholly within Smartcom's networks, thus minimizing the ability for a malicious intrusion at the network level. Smartcom encourages their customers to rigorously protect their internal networks from intrusion using firewalls and content filters. Obviously, any failure of a customer to do so would be outside of Smartcom's ability to control, however any identified misuse would subject the customer to service restrictions.
- 3) Through Smartcom's upstream long-distance carriers, monitoring of call volume to domestic and foreign destinations occurs on a 24-hour basis. Automatic blocking of excessive calling occurs and Smartcom's on-duty or on-call personnel are notified immediately so that the offending party can be identified and appropriate corrective actions taken, to include blocking of all call traffic from the offending customer if necessary.
- 4) Smartcom receives daily reports from our SIP monitoring software to identify calling trends and identify any obvious deviation from normal traffic levels. We also receive *instantaneous* alerts if our Call Per Second (CPS) threshold is breached at any time of the day or night, further allowing us to investigate the source of the abnormality.
- 5) All incoming traffic from our tandem partners is solely terminated within our footprint. Our switching system is set to disallow any tandem functionality of calls from an outside source.

Additionally, Smartcom Telephone, LLC (“Smartcom”) hereby certifies the following:

- Smartcom performs the following roles in the call chain: A Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users.
- Smartcom performs its STIR/SHAKEN obligations through a partner carrier (ANI Networks) as this carrier handles 100% of the outbound SIP traffic that we originate.
- Smartcom has not been prohibited from filing a certification in the Robocall Mitigation Database.
- Smartcom does not have a history of law enforcement, regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- Robocall Mitigation Primary Point of Contact:
- Howard L Hawbaker, Operations Director

admin@sctel.co
956 213-2040
600 Ash Ave
McAllen, TX 78501

In summary, Smartcom Telephone LLC is taking reasonable, technically-feasible steps to prevent and/or identify any misuse of originating call traffic. We will fully cooperate with any traceback investigations present to us in a timely manner. We welcome any input that you may have to further our goals of preventing illegal or unwanted call traffic.