

JSI LogicomUSA, LLC (FRN 0036873164)
formerly CRAM Industries, LLC dba LogicomUSA (FRN 0026466813)
Robocall Mitigation Plan

JSI LogicomUSA, LLC (“Company”) formerly CRAM Industries, LLC dba LogicomUSA provides wholesale VoIP solutions for retail service providers, herein after referred to as VoIP Partners, including over-the-top VoIP solutions for alternative voice providers such as Electric Cooperatives and municipalities. In addition to implementing STIR/SHAKEN on our network we have chosen to employ a multi-layered approach to address and mitigate illegal robocalling and the potential for originating, transporting, or processing of illegal robocalls, and to fully participate in industry call trace back efforts. In support of our STIR/SHAKEN compliance we have entered into an agreement with STI-PA and utilize TransNexus, Inc. as our STI-CA. Additional Company efforts include:

- Incorporation of robocall mitigation language into our contracts, terms of service, acceptable use policy, and/or other documents as appropriate prohibiting use of our platforms/services to make or receive illegal or fraudulent calls. Company requires business identification information to be provided prior to entering a contract for services including Federal Tax ID information, an FCC Form 499 Filer ID, and a Federal Registration Number (“FRN”) amongst other validation information.
- Specifically, with respect to VoIP Partner subscriber caller-ID information, to require that the caller-ID value be either a number assigned to the calling party, or one which the caller has the explicit permission of the assignee to use.
- When non-compliant calls come to our attention, through our own analysis or via our STI-CA services we promptly investigate and take necessary action with the offending customer to mitigate ongoing illegal activity.
- Company shall provide a point-of-contact for traceback and takedown requests from bona fide sources and respond within twenty-four (24) hours. For credible requests that include sufficient supporting detail, we will not require a subpoena or similar documentation.
- Company shall share as much information with industry forensics efforts and enforcement officials as is practical and legal, recognizing that users of our platform that are breaking the law need not be afforded the same privacy protections as those complying with the rules.
- Company shall exercise its due diligence by requiring our service vendors, including upstream provider partners, to implement these same practices and impose these same requirements, or face restrictions on their use of our platform/services, including, if necessary, complete termination of access.
- Company abuse mitigation practices shall be applied in a non-discriminatory manner.

- If we discover that traffic originally flagged as illegal is in fact legitimate, we will share that information with other parties in the call chain.
- Know Your Customer Vetting: Company requires its VoIP Partners to vet their end user subscribers thoroughly, with additional scrutiny of those subscribers involved with auto-dialed traffic types. Anonymous test accounts will not be provided to auto-dialers.
- Company will employ real-time controls on traffic. All calls must have valid caller-ID values, and for auto-dialed calls, each value must be checked against the list of numbers that customer provided and that Company staff vetted before establishing service. VoIP Partner subscribers must have a call-per-second limits commensurate with the traffic description provided.
- Company shall monitor, using state-of-the-art call analytics tools, the traffic moving through its network. CDRs are analyzed regularly including inspection of call durations, unusually large numbers of calls originating from the same number, excessive numbers of short duration calls and single ring call attempts. We detect, track and trend calling numbers as invalid, unallocated, or Do Not Originate (“DNO”). We verify frequent Caller-IDs to identify if any are being misused. When call analytics trigger a mitigation intervention event our VoIP Partner is contacted for further investigation. We complete the investigation cycle by documenting within our ticketing system the resolution and/or next steps.
- Utilizing the services of our STI-CA we to check the Certificate Revocation List (CRL) as part of routine compliance activities.
- Company has identified a single point of contact in charge of responding to all traceback requests made by ITG, law enforcement, and government agencies responsible for investigating suspected illegal robocalls originated by or passed to Company. Further we will respond to traceback requests fully and within twenty-four (24) hours as well as work with, communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling. Update the state Attorneys General about potential additional solutions for combatting illegal robocalls.
- Company has knowledge of all the upstream providers from which it receives traffic and has vetted these providers policies and protocols related to identifying and blocking illegal robocall traffic.
- For VoIP Partner’s residential subscribers Company makes available free, easy-to-use call blocking tools and regularly engage in easily understandable outreach efforts to notify VoIP Partners and their subscribers about these tools. For all types of VoIP Partners, Company implements network-level call blocking at no charge. We use best efforts to ensure that all tools offered safeguard personal, proprietary, and location information.
- Company uses best efforts to confirm the identity of new commercial customers on our network by collecting information from our VoIP Partners such as physical business location,

contact person(s), state or country of incorporation, federal tax ID, and understanding the nature of the customer's business including if/how they will employ auto-dialers or other robocall style tools in the conduct of their business.

- We monitor, through our Regulatory Compliance Department, the efforts of the Federal Trade Commission and the Federal Communication Commission in regard to their robocall mitigation efforts, identification of industry trends, provision of consumer education materials, and other related information and alerts.

Effective September 10, 2025
Version 4