



LCS Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by London Computer Systems, Inc (hereafter LCS). 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 LCS’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. LCS 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 LCS commits to responding within 24 hours 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 illegal robocallers that may use LCS’s service to originate calls. All calls originating on LCS’s network are subject to this robocall mitigation plan.

The following list spells out the methods used in the LCS Robocall Mitigation Plan

I. STIR-SHAKEN IMPLEMENTATION STATUS

As of 02/04/2026 LCS has fully implemented STIR-SHAKEN for all calls originating from equipment within our control.

II. CUSTOMER TERMS OF USE RESTRICTIONS

LCS end users subject to restrictions contained in our published legal notices and all executed contracts include requirements that VoIP services are provided pursuant to the Terms of Use requirements. Terms of Use stipulate, among other things, that customers are bound by and will comply with all FCC rules and regulations as well as State and Federal laws prohibiting illegal robocalls. LCS reserves the right and authority within our service agreements to suspend or terminate any customer’s service for violating applicable terms.

III. KNOW YOUR CUSTOMER (KYC) VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its network, LCS will use best practices in vetting the identity of all customers whether residential or commercial. The customer vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship.

Generally, LCS confirms the identity of customers using our services by collecting information such as:

- Physical customer location (Address)
- Contact Person(s) having authority to act on behalf of the customer.
- Contact information for the customer and the designated contact including
 - Phone Number
 - Email Address
- State of Incorporation for incorporated customers.
- Federal Tax ID (SSN for sole proprietorship OR EIN for incorporated businesses)
- A description of the nature of the customer's business

LCS further attempts to confirm the identity of the customer by comparing the information provided to publicly available information online. Suspicious patterns of behavior are flagged and reviewed at several points through the sales and onboarding process. If suspicious patterns are detected that exceed internal risk thresholds, LCS will terminate the sales or onboarding process of that customer.

LCS vets customers as part of the provisioning process and includes determinations on how many resources should be made available to the customer. Resource requests such as Line Limit and assigned Phone Numbers are compared against the stated business nature and intended use for consistency. Customers requesting many resources or resources that appear inconsistent with their size and use case are viewed as having higher risk and may be subject to additional review such as a more stringent background check and deeper review of available online resources to confirm the nature and validity of their business. LCS does not allow access to any resources until appropriate onboarding processes are completed.

Further, many of LCS's customers have a prior long-standing relationship with LCS using our Rent Manager software package. By the nature of these business interactions, we have a confirmed relationship including payments, billing addresses and direct contact details for key leadership and decision-making roles within our customer's organization.

IV. KNOW YOUR UPSTREAM PROVIDER

LCS has longstanding relationships with our upstream providers. LCS maintains regular contact with our providers and works quickly to respond to any requests

from our providers. Included in Appendix A of this document is a list of our upstream providers with contact information.

V. ONGOING ROBOCALL MITIGATION PRACTICES

LCS monitors network traffic at all times and mitigates or blocks suspicious traffic through automated methods and manual review.

1. LCS utilizes technology within OpenSips to identify and block associated SIP users for patterns such as:
 - a. register and invite patterns that are suspicious such as brute force attacks.
 - b. call patterns that are suspicious such as rapid calls or multiple simultaneous INVITE attempts or multiple ongoing calls.
2. LCS utilizes technology at our application layer to identify potential abuse and block associated SIP users such as
 - a. Attempts for multiple devices to register simultaneously with the same SIP credentials.
 - b. Registers that do not have an appropriately validated certificate from the physical phone vendor (Poly)
 - c. SIP requests from multiple locations for the same credentials.
3. LCS tracks information in detail for all calls including the SIP traffic flow using Homer.
4. LCS keeps detailed records of each outbound call including the IP address used to register the SIP user that initiated the call.
5. LCS utilizes monitoring of overall traffic and requests using Graylog and Grafana to identify suspicious spikes in traffic or other unusual patterns.
6. LCS monitors network layer traffic at a low level to identify potentially fraudulent behavior including monitoring for brute force attacks on our SIP network.
7. LCS has obtained a SOC 2 Type 2 attestation in which an independent audit has been conducted by Clark Schaefer Hackett to evaluate both the design and effectiveness of our physical security including validating best practices for data handling, source code changes, and organizational best practices.
8. LCS conducts regular internal and external third-party audits to assess the overall security of our digital systems.

LCS works with our upstream providers to respond to automated notifications that identify suspicious behavior through thorough investigation of each notification and a response to the provider detailing our investigation and the outcome.



LCS does not utilize any other external vendors or third-party solutions hosted outside of our systems to identify suspicious traffic.

Appendix A

Providers

Lumen Chris Wolsey Customer Success Advocate 385-295-9150	Sinch / Inteliquent Chet Zielinski Regional Vice President, Communication and Application Provider (CAP) Sales 216-373-4879
--	--

Traceback Request Single Point of Contact:

Name: Tony Little
Title: CTO
Phone Number: 513-583-1482
Email Address: tony@lcs.com