



Robocall Mitigation Plan

ICON Cloud Solutions, LLC (ICS) is committed to cooperating with the Federal Communications Commission (FCC), law enforcement and industry traceback consortium in investigating and stopping illegal robocallers.

ICS has instituted the following elements as part of our Robocall Mitigation Plan and Compliance. ICS is an Interconnected VoIP service provider servicing North America. This document contains information on the practices and procedures to mitigate and correct any occurrence of suspected fraudulent originating call activity.

Our hosted services qualify as full compliance for Stir/Shaken as we control both the customer telephone numbers and the originating equipment. ICS has implemented comprehensive STIR/SHAKEN protocols in addition to robocall mitigation measures.

ICS has never been subject to any Commission, law enforcement or regulatory agency action or investigation related to suspected unlawful robocalling of spoofing activities.

1. ICS Commitments include

1.1. Originating Call Certification

ICS certifies that all calls originating over our network are subject to robocall mitigation program.

1.2. Rapid Response (24 Hour)

ICS is committed to fully responding within 24 hours to Traceback Requests from the Industry Traceback Group (ITG) and civil and criminal law enforcement agencies pursuant to the requirements stated with the Seventh Call Blocking Order amendment to section 64.6305. We will cooperate fully to investigate and eliminate illegal robocalls from our services. When notified by TRG and/or FCC Enforcement Bureau ICS will block the identified illegal traffic.

1.3. Robocall Mitigation and Full Stir/Shaken Implementation

ICS is committed to enforcing robocall mitigation and the full deployment of STIR/SHAKEN to prevent the origination and receipt of illegal calls on our network.

1.4. Illegal Traffic Mitigation

ICS is committed to taking action to mitigate illegal traffic upon receiving formal notification from the FCC and law enforcement agencies.

1.5. Provider Notification

ICS is committed to working within our systems and our backhaul providers to refuse traffic from providers that are not registered in the Robocall Mitigation Database (RMD)

1.6. Implementation of DNO Lists



icon cloud solutions

ICS is committed to utilizing Do Not Originate (DNO) lists with information provided through both internal tools and those provided by our third party carries and ITG lists to block unauthorized numbers from originating and/or terminating calls

1.7. Customer Due Diligence and KYC:

ICS, requires by agreement that users of our services be registered as well as vigilant with regards to fraudulent activity, inclusive of robocall activity.

1.1. Customer Compliance

Each customer contractually agrees to immediately notify ICS in the event of the occurrence of such activity.

“Customer agrees to immediately notify ICS of any fraudulent activity, robocall activity or unauthorized use of its Services and/or equipment when they become aware of such activity.”

1.2. Customer Registration Information

Each customer and user of our services is registered as the direct user of the lines assigned to them. The registration includes the company’s legal name, civic address, authorized contact and federal tax ID. Prior to line porting on our service, we go through a vetting process to understand the use case of their contracted telephony service and line usage. Also, the customer must comply with Know Your Customer (KYC) vetting information.

1.8 Robocall Mitigation Certification: ICS is committed to providing call authentication of originating calls from our equipment to support our STIR/SHAKEN policies. ICS provides a certificate on our call traffic identifying the attestation level of each call.

2. System Monitoring

ICON Cloud Solutions backhaul providers utilize Robocall Mitigation software which provides call behavior analytics to identify suspicious call activity and calling patterns. ICS also manages call detail records for each customer identifying calling from numbers and destinations.

ICS monitors call traffic from each customer location to recognize irregular calling patterns. Should we see unusual call activity we will investigate the case and take the appropriate action in identifying the usage and then suspending services should it be necessary.

3. System Controls/Restrictions

All direct ICS customer systems are programmed and managed by ICS. ICS confirms that all systems are programmed to send the correct Caller ID and to only send numbers that are registered to the customer account. End users do not have access to program Caller ID information, this is controlled by ICS.

All ICS customers are restricted from using the ICS telephone system for any type of Robo calling though our customer service agreement and policy.



Call detail for trace back is provided by our back haul carriers. If ICS identifies and confirms a customer is performing Robo calls, ICS will take action to block and suspend calling or terminate the service agreement for the offending customer.

ICS utilizes third party tools such ALE 8770 and other for tracing calls.

ICS has confirmed that each of our upstream providers have implemented RMD policies and adhere to *STIR/SHAKEN* to prevent the origination and receipt of illegal on our network.

4. Controls Responsibility Compliance

ICS has a centralized group responsible for monitoring fraudulent communication activity. A specific email address, reportfraud@iconcloud.com, has been established for end users and outside parties to report suspected fraudulent calling activity such as robocalling. Additionally, users can initiate a call blocking request or an alert of suspected fraudulent activity via our website at www.iconcloud.com or directly by calling us 972-786-9000.

Robocall Call Responsible Party

ATTN: ICON Cloud Compliance Team
ICON Cloud Solutions, LLC
480 Wrangler Dr, Suite 400
Coppell, TX 75019
972-786-9000
reportfraud@iconcloud.com

5. Mitigation Response Steps

ICS's compliance team is committed to tracing calls when these reports have been received and then restricting such service as may be required. We have systems in place both within our switching architecture and backhaul services to block calls suspected as illegal or fraudulent.

We take the following practical steps in response to notification of fraudulent call activity:

- We run an analysis on the reported incident(s) and determine if this traffic is indeed routing through our network. If this traffic is not routing through our network, we reach back out to the reporting party for more information and to determine next steps.
- If we determine that the traffic is fraudulent, we inform our back haul carriers of the suspected fraudulent activity and then we take measures on our equipment to block traffic from and to our network equipment. If it is determined that the traffic is not fraudulent, we will reach back to the reporting party for more information.
- After the determination that the traffic is fraudulent, we will inform the reporting party that we have taken measures to block the traffic.
- We are implementing the following additional processes:
 - Short Duration Call Detection
 - Calling and Called Number Unusual Patterns
 - Repeated Attempts to Invalid Numbers