

Corporate IT, LLC

ROBOCALL MITIGATION PROGRAM

Table of Contents

Table of Contents.....	2
I. PURPOSE OF THIS PROGRAM.....	3
II. DEFINITIONS.....	3
III. STATEMENT OF POLICY.....	4
IV. GENERAL POLICIES FOR ROBOCALL MITIGATION.....	4
A. Requirements of Company to Mitigate Illegal Robocalls	4
B. Legal vs. Illegal Robocalls	4
V. PROCEDURES FOR ROBOCALL MITIGATION	5
A. Contact.....	5
B. Subscriber Vetting	6
C. Service Agreements	8
D. Telephone Number Validation	8
E. Network Capacity Limitations	8 9
F. Network Monitoring.....	10
G. Do Not Originate	10
H. International Call Originators.....	10
I. Certification and Contact Updates	10
APPENDIX 1 Point of Contact	11
APPENDIX 2 Know Your Customer Doc	12

I. PURPOSE OF THIS PROGRAM

Corporate IT, LLC, on behalf of itself ("the Company"), established a Robocall Mitigation Program (Program), implementing the policies and procedures within this Program for the reduction of the origination of illegal robocalls. In addition to these policies and procedures, the Company commits to cooperating with the Federal Communications Commission ("FCC"), law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls.

II. DEFINITIONS

Frequently used terms throughout this Program shall be defined as follows, in conjunction with any and all definitions as identified in 47 CFR § 64.6300.

Customer: A service provider's subscriber, which may or may not be the ultimate End User of the telecommunications service.

End User: The entity ultimately consuming the telecommunications service and may include the End User's device used for placing the call.

Industry Traceback Consortium: The consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls as selected by the Commission pursuant to §64.1203.

Robocall Mitigation Database: A database accessible via the Commission's website that lists all entities that make filings pursuant to §64.6305(b).

Telecommunications Carrier: a person or entity that meets the definition of 47 U.S.C. 1001(8), including a person or entity that FCC finds that its service is a replacement for a substantial portion of the local telephone exchange service under 47 U.S.C. § 1008(B) (ii).

Voice Service: Any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan (NANP) or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934, as amended; and includes:

- (i) Transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine; and

- (ii) Without limitation, any service that enables real-time, two-way voice communications, including any service that requires Internet Protocol-compatible customer premises equipment and permits out-bound calling, whether or not the service is one-way or two-way voice over Internet Protocol.

This includes common carrier voice, interconnected Voice over Internet Protocol (VoIP), one-way VoIP, fax transmissions, and over-the-top voice services.

III. STATEMENT OF POLICY

It is the policy of this Company to comply with the letter and spirit of all laws of the United States, applicable state statutes, and rules and requirements of the FCC. The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires a voice service provider to implement robocall mitigation strategies to reduce the origination of illegal robocalls, including implementing the STIR/SHAKEN caller ID authentication technology in the IP portions of their phone networks as well as developing non-IP caller ID authentication solutions.

As a part of its Robocall Mitigation Program, the Company will:

- (i) Vet all potential new clients via process outlined in section V. B. below along with blocking all traffic that has a Called From number that is listed as a Do Not Originate number or is not an active NPA-NXX-A block in the LERG;
- (ii) Commit to respond to all traceback requests within a 24-hour time period; and (iii) File its Robocall Mitigation Program in the Robocall Mitigation database.

This Program constitutes the required policies and procedures to implement the Company's Robocall Mitigation Program. All officers, employees, or agents of the Company are required to follow the policies and procedures specified in this Program.

IV. GENERAL POLICIES FOR ROBOCALL MITIGATION

A. Requirements of Company to Mitigate Illegal Robocalls

All officers, employees, and agents of the Company understand and agree that they will follow strictly the applicable federal and state laws, court orders, FCC Regulations, and the Company's policies and procedures in carrying out the responsibilities as described in this Program.

B. Legal vs. Illegal Robocalls

Voice Service Providers are required to take reasonable steps to avoid originating illegal robocall traffic, as defined within the Telephone Consumer Protection Act (TCPA).

Pursuant to the TCPA, and for purposes of this Program, an illegal robocall is a call:

- To a landline that leaves a pre-recorded or artificial voice message for telemarketing purposes, without a customer's prior consent.
 - o Non-telemarketing calls to landlines, regardless of whether it is pre-recorded or an artificial voice message, are not considered illegal robocalls.
- To a wireless phone that leaves a pre-recorded or artificial voice message, or is made with autodialer equipment, without the customer's prior consent.

- o Calls to wireless phones do not need to be telemarketing in nature to constitute an illegal robocall; any telemarketing or information call made using the mechanisms above, and without prior consent, constitutes an illegal robocall.

The Company will implement its Program policies and procedures in an effort to reduce perceived illegal calls of the above types. If a customer claims that a call has been incorrectly flagged as an illegal robocall, the customer can notify the Company for a more in-depth determination as to the legality of the call(s) in question.

V. PROCEDURES FOR ROBOCALL MITIGATION

A. Contact

Pursuant to 47 CFR 64.6305(B)(4), the Company has designated a point of contact to receive notice of any incidents of illegal robocall traffic. This Point of Contact is named in Appendix 1 of this Program.

The Company will respond to all traceback requests within twenty-four (24) hours of receipt of the request, even if the investigation is ongoing, and will provide responsive information reasonably available at the time of the response. The Company maintains records sufficient to support traceback investigations and retains such records in accordance with applicable regulatory requirements and industry best practices.

If traceback investigations identify a customer whose traffic demonstrates a pattern consistent with illegal robocalling, the Company will promptly investigate and take appropriate mitigation measures, which may include enhanced monitoring, traffic restriction, suspension, or termination of service.

The President, or his designee, is responsible for overseeing timely response to traceback requests and ensuring appropriate follow-up actions are taken.

When the Company makes a verified determination of an illegal robocall originating from the Company's network, the following actions will be initiated:

1. The Company personnel will review the call information to determine whether the call is from the Company's network or one of its affiliates. If the call is from an entity other than the Company, the notice will be forwarded to that entity for review and any action or response.
2. The following actions may be taken with offenders:
 - a. If the offender is an employee, the supervisor responsible will be notified, and appropriate disciplinary action may be warranted. A copy of the violation will be filed by HR in the employee's personnel file.
 - b. If the offender is a customer, the customer will be notified by telephone and email of the offense. If it is a first-time offense, the customer will be notified and advised that an alleged violation has been received and that any further violations could affect the customer's account. Notification of a second offense will result in the same action. A third offense will result in notice that the customer's service has been restricted for ninety (90) days to limit the ability

to violate the law. A fourth offense will result in termination of service. Notwithstanding the above, the Company reserves the right to expedite termination of service.

In addition to the above actions the Company may take when it identifies a pattern consistent with illegal robocalls, the Company may also initiate or cooperate in a traceback investigation to verify that the originating customer owns or is authorized to use a Caller ID number. In conjunction with following Industry Traceback Group-recommended best practices, the Company maintains internal processes and system access necessary to respond promptly to traceback and trace-forward investigations.

Upon receipt of notice from the Company that an illegal robocall originated from customer's number, customer may dispute the determination.

1. If the customer's number has been inadvertently flagged as illegal robocalling due to third-party unauthorized spoofing of the customer's number, the Company will make a good faith effort to contact database vendors in an attempt to correct the issue.
2. If the robocall was a legal robocall originating from the customer, the circumstances of the robocall will be reviewed with the customer and the customer will be monitored for a thirty (30) day period thereafter.

B. Subscriber Vetting

The Company will vet the identity of large retail and wholesale subscribers, in conjunction with (i) approving applications for service; (ii) provisioning network connectivity; (iii) entering into any contract agreements; or (iv) granting the right-to-use telephone number resources. In its vetting process, Company will confirm the identity of new or renewing business customers by collecting information such as the following:

- (i) physical business location;
- (ii) a contact person for the business; (iii) state or country of incorporation; (iv) nature of customer's business.

The Company will complete an additional review of any outbound call centers or highvolume origination services within its network, including more stringent background checks and require completion of "Know Your Customer" document.

Know Your Customer

Corporate IT, LLC ("Corporate IT") is primarily a provider of domestic voice services to end-user customers that are existing customers of its IT services business. All of our voice services customers are personally known to us. Corporate IT, with respect to its network services company, only interconnects with US based entities for domestic US call origination and termination that have active 499 filer IDs, certified on the Robocall Mitigation Database.

Acceptable Use Policy

Before Corporate IT executes any agreement, customers must agree to the terms and conditions, including a commitment to comply with Corporate IT's Terms of Use. Among other things, these Terms prohibit:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive, or misleading, or any activity that exploits, harms, or threatens to harm children.
- Using Corporate IT's Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.
- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations

Corporate IT's customer MSA allows and authorizes Corporate IT to suspend and/or terminate all Services in any event of fraudulent practices including but not limited to an AUP violation.

Recurring Customer Reviews:

Periodic Wholesale Customer Review (if applicable):

- Purpose: To verify the status of any wholesale customer's 499 filer ID and Robocall Mitigation Database status.
- Objective: To ensure that such customers maintain required regulatory certifications.

Quarterly Customer Review:

- Purpose: To perform a comprehensive review of all wholesale, outbound call centers or highvolume origination services customers.
- Objective: This review involves an Internet search of each customers' company name and principals to ensure no negative allegations, lawsuits or other relevant information against customer has been made public since initial onboarding date.

Annual Customer Review:

- Purpose: The primary purpose of an annual review of KYC documents is to confirm the accuracy and validity of the customer's identity and information. It helps detect any discrepancies or changes that may have occurred over the course of the year and is crucial for regulatory compliance.
- Objective: The information on these documents is cross-referenced with the information stored in the customer's account. Any discrepancies or inconsistencies are flagged for further investigation.

Where an existing customer in good standing adds additional services under the same legal entity and ownership structure, the Company may rely on previously collected Know Your Customer documentation, provided that the customer's legal status, ownership, and anticipated traffic profile have not materially changed. The Company reserves the right to request updated documentation where changes in service scope or traffic profile warrant additional review.

C. Service Agreements

The Company maintains a document (e.g. Acceptable User Policy (AUP), Tariff, etc.) outlining the acceptable uses of the service and prohibits among other things:

- (i) modification of network information for deceptive purposes;
- (ii) violation of local, state, or federal laws; and
- (iii) use of the Company's network to engage in fraudulent activity.

The Company reserves the right to suspend or terminate any subscriber account for violating the service terms. The Company will also require a point of contact which can be contacted if needed for traceback cooperation in case illegal robocalling is detected.

D. Telephone Number Validation

A subscriber is permitted to use a telephone number as their caller identity if the number is directly managed by the Company and/or obtained by the Company via an underlying partner. Where equipment allows, the Company has established a process for ensuring subscribers are utilizing only telephone numbers assigned to them or otherwise authorized for use.

For subscribers with a single line service, the Class 5 switch is configured to apply a static outbound caller identification number assigned to that subscriber at the time of service origination, for both services connected via TDM or IP. Subscriber-provided caller identification information is not utilized for these single line services. This configuration provides an automated and secure means of ensuring that only the caller identification number assigned to that subscriber is presented on outbound calls and prevents the use of unauthorized caller identification numbers.

For subscribers with multi-line telephone systems (MLTS), for both services connected via TDM or IP, the Company screens all originating calls and compares the originating telephone number against the numbers assigned to that MLTS subscriber. If the originating number matches one of the numbers assigned to the subscriber, the call is permitted to proceed. If the subscriber seeks to originate a number that has not been directly assigned by the Company, the Company requires a Letter of Authorization (LOA) or other acceptable documentation reasonably demonstrating that the subscriber is authorized to use the number before applying full caller ID attestation. Where such documentation is not provided, the Company may permit the call to proceed but will limit caller ID authentication attestation consistent with its STIR/SHAKEN policy.

For both single line services and MLTS, this screening and validation process provides an automated and secure means of validating originating telephone numbers and enables the Company to cooperate fully with traceback efforts.

STIR/SHAKEN Attestation Policy

The Company implements STIR/SHAKEN caller ID authentication consistent with applicable FCC rules and industry standards. Attestation levels are applied as follows:

- (iv) Full (A) Attestation is applied when the Company has authenticated the originating customer and has verified that the calling number is assigned to, or otherwise authorized for use by, that customer.
- (v) Partial (B) Attestation is applied when the Company has authenticated the originating customer but cannot independently verify that the calling number is assigned to that customer.
- (vi) Gateway (C) Attestation is applied when the Company is acting as a gateway provider or does not have a direct authenticated relationship with the originating party.
- (vii) All Class 4 SIP traffic follows the Company's STIR/SHAKEN attestation policy as described above.

E. Network Capacity Limitations

The Company has reviewed the network capacity requirements for the two primary segments of the network, subscriber facing and PSTN facing, and has established appropriate capacity limitations to align with each service need. By limiting the capacity of each segment of the network based on service needs allows the Company to mitigate the risk of flooding the network with unintended calls, such that it is appropriately sized to minimize call blocking, but not allow excess calling capability that could be used to generate illegitimate traffic. These efforts protect both on-network and off-network subscribers to be able to traceback originating calls to their source.

For the subscriber facing segment of the network, when a new service is established the capacity requirements are discussed with each subscriber. For example, if providing service to a MLTS, the concurrent call capacity is determined by understanding the subscribers service needs such as how many end points will be used, average call usage and other metrics. This allows the Company to establish connectivity to MLTS that is right sized based on the subscribers need. This connectivity is capped by the Class 5 switch so no more concurrent calls than the identified number can originate. This concurrent call capacity is monitored and can be expanded by the subscriber when the service need is identified. In addition to limiting the capacity of originating calls for MLTS, the Company also limits the number of concurrent calls for individual lines based on the service need. This is accomplished within the Class 5 switch by restricting the number concurrent calls of each end point to the original subscriber service request. Similarly, this will not allow an unintended number of calls to originate from a subscriber.

For the PSTN-facing segment of the network, all interconnection trunk groups and connections to other service providers and interexchange carriers are limited to a concurrent call capacity sufficient to minimize call blocking, but not grossly oversized so as to create an opportunity to flood the PSTN with illegitimate traffic. These capacity limits are applied across trunk groups regardless of technology and are adjusted as thresholds are reached based on documented traffic patterns and service needs.

F. Network Monitoring

The Company has set up a recurring schedule for conducting a comprehensive network monitoring plan with the goal of identifying irregular calling patterns that may indicate potential illegal originating robocalls. The schedule and areas of the network being monitored for illegal originating robocalls are outlined below:

Interconnection Traffic Monitoring:

The Company has established a routine process of monitoring call volume and traffic patterns for originating traffic transmitted over its interconnection trunk groups and carrier interconnects. By monitoring this traffic over an extended period of time, the Company establishes baseline traffic patterns based on subscriber usage. If the Company identifies spikes or changes exceeding predefined engineering thresholds for a given trunk group or interconnection, further analysis is conducted to determine the source of the change.

This monitoring is conducted on a regular basis for this portion of the network.

If the Company's monitoring process identifies the potential of illegal robocalls originating from the network, the Company will follow the internal policy and procedure in accordance with this Program.

Local Monitoring:

The Company has deployed local monitoring tools based on the capabilities of the Class 5 switch. The Class 5 switch statistics allow the Company to monitor originating traffic for all trunk groups or traffic to a particular carrier. The data collected is able to provide reports that can include total originating calls and total originating call usage. By monitoring this traffic over an extended period of time, the Company has established a baseline for traffic patterns based on their subscriber's regular usage. If the Company notices spikes or changes greater than their predefined engineered threshold per trunk group, further analysis is conducted to identify the source of the change.

This monitoring is conducted on a regular basis for this portion of the network.

If concerns are identified for any individual line or MLTS, usage statistics can be used to further monitor that particular subscriber's service specifically. The Company can set up reports to monitor originating call attempts and originating call usage. This data can help set a baseline of normal traffic patterns and signal when abnormal traffic patterns are emerging in order to further investigate.

If the Company's monitoring process identifies the potential of illegal robocalls originating from the network, the Company will follow the internal policy and procedure in accordance with this Program.

Call Record Monitoring:

The Company processes call detail records on a nightly basis by exporting the data from the all switch platforms. These call records can be used to help identify the potential of illegal originating robocalls. If the Company becomes concerned with any subscriber based on the collective and comprehensive efforts

identified in this Program, the call records can be analyzed and summarized to flag traffic that has the characteristics of illegal originating robocall traffic.

The monitoring includes high call volumes, low duration calls, sequential dialing patterns, calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator and other evolving best practices as identified by the collective industry helping to combat identifying illegal robocalls.

Where equipment permits, the Company has deployed a monitoring/diagnostics tool as part of their switching network. This diagnostics tool provides detailed call traces suitable for the Company to diagnose, monitor and collect data associated with calls traversing the network. When the monitoring/diagnostics tools are enabled on the switching system, traces are recorded for all calls and transferred to an external database for future review. These traces do not have to be individually enabled on particular lines or subscribers and are always active. When investigating suspicious traffic, a web application is used to search the database for traces for particular lines or subscribers and to view the traces. The application also allows traces to be printed or exported for offline storage for further evaluation if required. The traces include decoded signaling messages, routing and number validation events, call service actions/decisions, codec selection, echo cancellation programming, media events such as digit and tone detection, tone generation, and digit out-pulsing, billing records and concise call logs. This collection of data allows for a comprehensive ability to monitor network traffic.

This monitoring is conducted on an as needed basis for specific subscribers suspected of illegal originating robocalls.

If the Company's monitoring process identifies the potential of illegal robocalls originating from the network, the Company will follow the internal policy and procedure in accordance with this Program.

G. Do Not Call Registry

The Company has implemented a policy that will block traffic from inactive NPANXX blocks as well as the ITG list of do not originate TN's.

H. International Call Originators

The Company may carry traffic that originates outside the United States through arrangements with upstream providers. The Company requires that any upstream provider comply with applicable FCC Robocall Mitigation Database requirements and STIR/SHAKEN obligations. The Company validates upstream provider status as part of its onboarding and periodic review process.

I. Company OCN

The Company's OCN is 870K.

J. Upstream Provider

The Company only uses upstream providers for domestic US traffic that are listed in the RMD and maintains a robust fraud detection system. In addition, any upstream provider must possess the ability to connect, in real time, with the Company so that issues with calls being processed by the Company can be immediately identified and addressed.

K. Stir/Shaken Implementation

The Company registered with Neustar, a third-party provider, to obtain their own unique token. The Company's traffic is either signed directly by the Company or the Company's sign is implemented by the Company's upstream provider such that the Company's sign is located in the call stream for easy identity.

L. Position in Call Chain

The Company's position in the call chain is typically the end-user's service provider.

M. Certification

Except as to periodic traceback requests, the Company has not been subject to a Commission Law Enforcement, or regulatory action or investigation due to suspected unlawful robocalling or spoofing.

N. Certification and Contact Updates

As required, the Company will submit any necessary updates because of changes to the Company certification, identification information, or contact information to the Commission within (10) business days of the change. The Company shall complete annual recertification of its Robocall Mitigation Database filing no later than March 1 of each year and shall retain documentation evidencing such recertification for a minimum of five (5) years. The President, or his designee, is responsible for ensuring timely completion of such filings and recertifications.

APPENDIX 1
Point of Contact

Pursuant to 47 CFR 64.6305(B)(4), the Company hereby designates the following senior officer or employee to serve as the Point of Contact for notification of illegal robocalls.

PRIMARY CONTACT: Joseph Nativ

TITLE: President ADDRESS: 23800 Northwestern Hwy Ste 190B Southfield MI 48075

E-MAIL ADDRESS: office@corpit.xyz