

Robocall Mitigation Plan

Section I: Introduction and Statement of Policy

A. Preamble

This document constitutes the official Robocall Mitigation Plan ("the Plan") for Civilization Systems LLC, a Delaware Limited Liability Company, doing business as Essential Tech Support ("the Company"). This Plan is established and maintained in strict accordance with the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act and the rules promulgated thereunder by the Federal Communications Commission ("FCC"), specifically as codified in Title 47 of the Code of Federal Regulations, Section 64.6305 (47 CFR §64.6305).¹ This Plan details the affirmative, effective measures and "reasonable steps" the Company implements to prevent the origination, carrying, or processing of illegal robocall traffic on its network. It serves as a foundational component of the Company's certification in the FCC's Robocall Mitigation Database (RMD).²

B. Statement of Unwavering Commitment

Civilization Systems LLC maintains a zero-tolerance policy for the use of its network and services for the transmission of illegal robocalls. The Company is fundamentally committed to protecting the integrity of the public switched telephone network (PSTN), safeguarding consumers from fraudulent and abusive communications, and upholding all applicable federal and state telecommunications laws and regulations.³ The principles and procedures outlined in this Plan are not merely compliance obligations; they represent a core operational priority integrated into every aspect of the Company's network management, customer relations, and corporate governance.

C. Scope and Applicability

The provisions of this Plan are universally applicable and legally binding upon all employees, contractors, agents, and customers of Civilization Systems LLC. Adherence to this Plan is a material term of the Company's Acceptable Use Policy (AUP) and is incorporated by reference into all customer service agreements, interconnection agreements, and terms of service. Any violation of this Plan by a customer or affiliate is considered a material breach of their service agreement and will subject the violator to immediate remedial action, up to and including the suspension or termination of service and reporting to law enforcement authorities.

D. Definition of Terms

For the purposes of this Plan, the following terms shall have the meanings ascribed to them below, consistent with FCC definitions ⁴:

- **Illegal Robocall:** A call made with an automatic telephone dialing system or a prerecorded or artificial voice that is not in compliance with the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, or other applicable federal and state laws.
- **Voice Service Provider:** Any entity that furnishes voice communications to an end user using resources from the North American Numbering Plan (NANP) and is interconnected with the PSTN.⁴ Civilization Systems LLC operates as a Voice Service Provider.
- **Gateway Provider:** A U.S.-based provider that receives traffic from a foreign provider and transmits it to another provider within the United States.
- **Intermediate Provider:** Any entity that carries or processes traffic that traverses the PSTN at any point, insofar as that entity neither originates nor terminates that traffic.⁴
- **Traceback:** The process of identifying the source of illegal or unwanted robocalls by tracing the call path back from the recipient to the originator.
- **STIR/SHAKEN:** The Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN) framework for authenticating and verifying caller ID information for calls carried over Internet Protocol (IP) networks.
- **Robocall Mitigation Database (RMD):** A database administered by the FCC where all voice service providers must file certifications detailing their robocall mitigation efforts.²

Section II: Program Administration and Responsible Personnel

A. Designation of Robocall Mitigation Officer

To ensure clear accountability and facilitate rapid response to regulatory and law enforcement inquiries, Civilization Systems LLC has designated a single point of contact responsible for the oversight, implementation, and enforcement of this Plan. This designation fulfills the FCC's requirement for a named individual responsible for addressing robocall mitigation-related issues.⁶

- **Name:** Vanessa Holub
- **Title:** COO
- **Department:** Operations
- **Business Address:** 822 Guilford Ave #126, Baltimore, MD, 21202
- **Telephone Number:** 1-410-921-2921
- **Email Address:** vanessa@civsys.it

B. Duties and Responsibilities

The structure of the Company's compliance program centralizes responsibility with the designated officer to prevent the diffusion of duties that can lead to missed deadlines or incomplete responses, particularly concerning the critical 24-hour traceback window. This organizational choice is a direct procedural safeguard designed to ensure consistent and timely compliance. The duties and responsibilities of the Robocall Mitigation Officer include, but are not limited to:

- Serving as the exclusive and direct point of contact for all robocall mitigation-related communications, including traceback requests, from the FCC, federal and state law enforcement agencies, and the industry traceback consortium.
- Managing the entire lifecycle of traceback requests, from receipt and acknowledgment to investigation and timely response, ensuring strict adherence to the 24-hour response commitment detailed in Section IV of this Plan.
- Overseeing the rigorous customer and upstream provider due diligence processes detailed in Section III.A to prevent bad actors from gaining access to the Company's

network.

- Conducting periodic reviews and updates of this Plan to ensure it remains current with evolving FCC regulations, emerging industry best practices, and new threat vectors.
- Developing and coordinating mandatory internal training programs for all relevant personnel on the Company's robocall mitigation policies and their specific responsibilities thereunder, as described in Section V.B.
- Authorizing and directing any necessary remedial actions against customers found to be in violation of this Plan, including service suspension or termination.

Section III: Detailed Robocall Mitigation Program: Specific Reasonable Steps

This section constitutes the substantive core of the Plan, detailing the affirmative and effective measures the Company takes to prevent illegal robocalls. These measures are designed as a multi-layered defense system, creating a high barrier to entry for malicious actors and enabling rapid detection and mitigation of any illicit traffic that may appear. This systematic approach is a direct response to FCC mandates requiring a detailed description of the "specific reasonable steps" a provider has taken to avoid originating illegal traffic.⁶

A. Customer and Upstream Provider Due Diligence ("Know Your Customer/Upstream")

A foundational element of the Company's mitigation strategy is a rigorous due diligence program designed to confirm the identity, legitimacy, and business practices of any entity seeking to interconnect with its network. This program directly addresses the FCC's "know its customers" and "know its upstream providers" requirements.⁸

1. Procedures for New Customers (KYC)

The Company will not provide service to any customer until the following multi-stage onboarding process is successfully completed:

1. **Information Collection:** The Company mandates the collection of comprehensive and

verifiable information from all prospective customers, including:

- Legal business name and all "Doing Business As" (DBA) names.
 - Certified articles of incorporation or other official business formation documents.
 - Federal Employer Identification Number (EIN) or, for non-U.S. entities, an equivalent government-issued tax or business identifier.
 - The physical address of the primary place of business. Post office boxes or virtual office addresses are not acceptable as the sole business address.
 - The full names, titles, and direct contact information (email and phone number) for key personnel, including the Chief Executive Officer, Chief Technology Officer, and a designated compliance contact.
 - A detailed and transparent description of the customer's business model and the specific, intended use of the Company's voice services. This includes the nature of expected call traffic (e.g., transactional notifications, customer support, marketing) and expected call volumes.
 - A mandatory disclosure of any formal FCC, Federal Trade Commission (FTC), law enforcement, or other regulatory agency action or investigation within the prior two years related to suspected illegal robocalling, spoofing, or deficiencies in an RMD certification.⁷
2. **Verification:** The Robocall Mitigation Officer or their designee will independently verify the collected information. This verification process includes cross-referencing information with public records databases (e.g., Secretary of State business filings), utilizing third-party business verification services, and, where necessary, direct communication with the customer's principals.
 3. **Risk Assessment:** Upon successful verification, each prospective customer is assigned a risk profile. Factors influencing this profile include the customer's business model (e.g., high-volume outbound calling campaigns are considered higher risk), the jurisdiction of operation, and the results of the verification process. Customers classified as high-risk are subject to enhanced monitoring and lower traffic thresholds upon activation.

2. Procedures for Upstream Providers (Know Your Upstream)

The Company will only interconnect with and accept traffic from upstream providers that demonstrate a commitment to robocall mitigation. The Company's procedures include:

1. **RMD Verification:** The Company will not accept traffic directly from any provider that is not validly registered and in good standing in the FCC's Robocall Mitigation Database. The status of all upstream partners will be verified prior to interconnection and re-verified on a periodic basis.¹
2. **Due Diligence:** The Company will conduct due diligence on all potential upstream providers commensurate with the KYC process detailed above, ensuring they are

legitimate, established entities with transparent robocall mitigation practices.

B. Contractual Covenants and Prohibitions

All service agreements between Civilization Systems LLC and its customers contain explicit, legally binding provisions that prohibit the use of the Company's network for unlawful purposes. These contractual measures create a clear legal basis for enforcement and ensure that customers are fully aware of their obligations.⁹ Service agreements will include, at a minimum, the following clauses:

1. An explicit prohibition against originating any calls that violate the Telephone Consumer Protection Act (47 U.S.C. §227), the Truth in Caller ID Act (47 U.S.C. §227b), FCC regulations, or any other applicable federal or state laws.³
2. A requirement for the customer to cooperate fully, transparently, and promptly with any traceback investigation initiated by the Company, the FCC, law enforcement, or the industry traceback consortium.
3. A binding warranty from the customer that they have obtained the requisite prior express written consent for all autodialed or prerecorded voice message calls delivered to wireless numbers and for all telemarketing calls delivered via prerecorded message to residential lines.
4. An unambiguous clause granting the Company the absolute right to monitor the customer's traffic for patterns indicative of illegal robocalling and to immediately suspend or terminate service, without prior notice or liability, if the Company forms a reasonable belief that a violation of its policies or the law has occurred or is occurring.¹⁰

C. Network Monitoring and Traffic Analysis

The Company employs a proactive, technology-driven approach to network monitoring, recognizing that real-time analysis is essential for the early detection and mitigation of illegal robocall campaigns. This addresses the FCC's requirement that providers describe the analytics systems they use to identify and block illegal traffic.⁸

1. **Analytics System:** The Company utilizes a sophisticated call analytics and fraud detection platform to monitor its network.
 - **Vendor Identification:** The Company's call analytics and traffic monitoring are managed using the following platform(s):.⁶
 - **Monitored Metrics:** The system analyzes Call Detail Records (CDRs) and Session

Initiation Protocol (SIP) signaling data in real-time. It is configured to detect and flag anomalies and patterns highly correlated with illegal robocalling, including but not limited to:

- Sudden, significant spikes in call attempts from a single customer account or IP address, particularly from new accounts.
 - An abnormally high percentage of short-duration calls (e.g., under 15 seconds), which can indicate mass dialing campaigns hitting voicemail systems.
 - Consistently low Answer-Seizure Ratio (ASR) or Average Call Duration (ACD), suggesting that calls are unanswered or quickly terminated by the called party.
 - Sequential dialing patterns (e.g., calls to a block of numbers in numerical order).
 - The use of invalid, unallocated, or high-risk numbers in the Caller ID field.
2. **Alerting and Response:** When the analytics system detects activity that breaches predefined thresholds or matches known robocalling patterns, an automated alert is immediately generated and sent to the Robocall Mitigation Officer and the network operations team. This triggers an immediate investigation. The responsible customer may be contacted to provide an explanation for the anomalous traffic. If a satisfactory explanation is not provided or the traffic is determined to be illicit, the account will be immediately suspended pending further review or termination.

D. Affirmative Call Blocking and Mitigation Technologies

In addition to monitoring and analysis, the Company implements specific technologies and processes to affirmatively block calls that are highly likely to be illegal before they exit the network.¹¹

1. **Do Not Originate (DNO) Lists:** The Company subscribes to and enforces industry-recognized and internally managed DNO lists. These lists contain telephone numbers that should never be used as an originating Caller ID, such as numbers assigned to government agencies (e.g., IRS, FCC), financial institutions, public safety answering points (PSAPs), and known inbound-only lines. Any outbound call attempt from the Company's network that spoofs a number on a DNO list is automatically blocked.
2. **Dynamic Blacklisting:** The Company maintains a dynamic blacklist of telephone numbers, IP addresses, and other identifiers that have been confirmed as sources of illegal robocalls through traceback requests, credible complaints, or internal monitoring. All traffic originating from a source on this blacklist is blocked by default.
3. **Invalid Number Blocking:** The Company's platform is configured to block any call originating on its network that attempts to use a calling party number that is invalid under the North American Numbering Plan (NANP), such as numbers with an invalid area code (e.g., 000, 123) or unassigned number ranges.

Section IV: Traceback Compliance and Law Enforcement Cooperation

Rapid and effective cooperation with traceback efforts is the lynchpin of the industry-wide campaign against illegal robocalls. It allows regulators and law enforcement to quickly identify and pursue bad actors. The Company views its traceback obligations as one of its most critical compliance functions and has structured its internal procedures to guarantee adherence to the FCC's strict deadlines.¹

A. Unconditional Commitment to Traceback Response

In accordance with 47 CFR §64.6305(d)(iii), Civilization Systems LLC makes the following unconditional commitment:

"Civilization Systems LLC commits to responding fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service."¹

B. Internal Traceback Procedure

To ensure the foregoing commitment is not merely a statement but an operational reality, the Company has implemented a detailed internal procedure for handling all traceback requests. This workflow is designed to ensure speed, accuracy, and accountability.

1. **Receipt and Triage:** All traceback requests are directed to the dedicated email address monitored continuously by the Robocall Mitigation Officer. Upon receipt, the request is logged, and an acknowledgment of receipt is sent to the requesting entity within one (1) hour.
2. **Investigation:** The Robocall Mitigation Officer immediately initiates an investigation, using network logs, CDRs, and other platform data to trace the call identified in the request back to its source within the Company's network. This process identifies the

specific customer account and, if applicable, the originating IP address responsible for the call.

3. **Reporting:** A complete and accurate response is compiled and transmitted to the requesting entity. This response will identify the upstream source of the call on the Company's network. This entire process, from receipt to response, is managed to ensure completion well within the mandated 24-hour window.
4. **Remediation:** Concurrent with the traceback response, the Robocall Mitigation Officer initiates internal remediation procedures. Based on the findings, this may include issuing a formal warning to the responsible customer, immediately suspending the customer's account to prevent further illicit traffic, or proceeding with permanent termination of service and reporting the customer to law enforcement.

Section V: Policy Publication, Training, and Maintenance

A compliance program is only effective if it is transparent, understood by those who must execute it, and maintained to reflect the current regulatory landscape. This Plan is therefore treated as a living document, subject to ongoing review and dissemination.

A. Public Accessibility

In the interest of transparency, Civilization Systems LLC will publish the current version of this Robocall Mitigation Plan in a conspicuous and readily accessible location on its public-facing website, essentialtechsupport.com. This ensures that regulators, upstream and downstream partners, and the public can review the Company's stated policies and commitments.¹⁰

B. Internal Training

A policy is ineffective without proper training. All Company employees and contractors with roles related to sales, customer onboarding, network operations, and compliance will receive mandatory training on this Plan. This training will occur upon hiring and will be refreshed on at least an annual basis. The training will cover the specific responsibilities of each role in

upholding the Plan, such as identifying red flags during customer vetting, recognizing suspicious traffic patterns, and understanding the critical importance of the traceback procedure.

C. Plan Review and Updates

The dynamic nature of both robocalling threats and FCC regulations necessitates a proactive approach to policy maintenance. The Robocall Mitigation Officer is responsible for reviewing this Plan at least annually. A review will also be triggered by any significant event, such as a new FCC Report and Order on robocalling, the discovery of a new threat vector, or any internal compliance incident. Any material changes to the Company's mitigation practices as described herein will be reflected in an updated version of this Plan. The Company commits to updating its filing in the FCC's Robocall Mitigation Database within 10 business days of any such material change, as required by 47 CFR §64.6305(d)(5).⁶ This procedural safeguard is designed to prevent the Company's RMD certification from becoming deficient or outdated, a known cause for FCC enforcement actions.⁸

Appendix A: Regulatory Compliance Matrix

To facilitate efficient review and demonstrate the comprehensive nature of this Plan, the following matrix maps the specific requirements for a voice service provider's robocall mitigation program description under 47 CFR §64.6305(d) to the corresponding sections of this document. This tool provides a clear, at-a-glance cross-reference, confirming that every regulatory mandate has been explicitly addressed.

47 CFR § 64.6305(d) Requirement	Corresponding Section in This Plan	Summary of Compliance Measure
(d)(ii) Description of the specific reasonable steps taken to avoid originating illegal robocall traffic.	Section III	The Plan details a multi-layered program including rigorous KYC, binding contractual prohibitions, real-time network monitoring, and affirmative call blocking.

(d)(ii) Description of compliance with "know your customer" obligations.	Section III.A	Details a mandatory information collection and verification process for all new customers to confirm identity, legitimacy, and intended use of service.
(d)(ii) Description of call analytics system(s) used to identify and block illegal traffic, including the name(s) of any third-party vendor(s).	Section III.C	Specifies the use of [Placeholder: Vendor Name or "a proprietary system"] to analyze CDRs and signaling data for patterns indicative of illegal robocalling, triggering alerts and investigation.
(d)(iii) A statement of the voice service provider's commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.	Section IV.A	Provides a clear, unconditional, and verbatim statement of commitment to the 24-hour traceback response requirement.
(d)(iii) A statement of commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use its service.	Section IV.A & IV.B	Includes the explicit statement of cooperation and is supported by a detailed internal procedure for investigating traceback requests and taking remedial action against offending customers.
Requirement to designate a contact person responsible for addressing robocall mitigation-related issues, including name, title, and contact information.	Section II	Formally designates a Robocall Mitigation Officer and provides all required contact information, centralizing responsibility and ensuring a single point

(Derived from (d)(4)(v) in full rule text).		of contact for regulators.
---	--	----------------------------

Works cited

1. 47 CFR 64.6305 -- Robocall mitigation and certification. - eCFR, accessed August 30, 2025, <https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-HH/section-64.6305>
2. Robocall Mitigation Database - Federal Communications Commission, accessed August 30, 2025, <https://www.fcc.gov/robocall-mitigation-database>
3. FCC and State AG Announcements Show Focus on Robocall Enforcement, accessed August 30, 2025, <https://www.kelleydrye.com/viewpoints/blogs/ad-law-access/fcc-and-state-ag-announcements-show-focus-on-robocall-enforcement>
4. Caller ID Authentication... - Federal Communications Commission, accessed August 30, 2025, <https://docs.fcc.gov/public/attachments/DA-21-724A1.docx>
5. What is the FCC's Robocall Mitigation Database? - TEC Services Group, accessed August 30, 2025, <https://www.tecsg.com/what-is-the-fccs-robocall-mitigation-database/>
6. Federal Communications Commission § 64.6305 - GovInfo, accessed August 30, 2025, <https://www.govinfo.gov/link/cfr/47/64?link-type=pdf&ionnum=6305&year=mostrecent>
7. 47 CFR § 64.6305 - Robocall mitigation and certification. - Legal Information Institute, accessed August 30, 2025, <https://www.law.cornell.edu/cfr/text/47/64.6305>
8. Federal Communications Commission, accessed August 30, 2025, <https://docs.fcc.gov/public/attachments/DA-25-737A1.pdf>
9. All Providers Must Submit Expanded Filing in Robocall Mitigation Database by February 26, 2024 - Lerman Senter, accessed August 30, 2025, <https://www.lermansenter.com/all-providers-must-submit-expanded-filing-in-robocall-mitigation-database-by-february-26-2024/>
10. Robocall-Mitigation-Plan.pdf
11. Robocall mitigation - TransNexus, accessed August 30, 2025, <https://transnexus.com/robocall-mitigation/>
12. Code of Federal Regulations Title 47. Telecommunication 47 CFR § 64.6305 | FindLaw, accessed August 30, 2025, <https://codes.findlaw.com/cfr/title-47-telecommunication/cfr-sect-47-64-6305-nr3/>
13. FCC Removes Voice Service Providers from Robocall Mitigation Database, accessed August 30, 2025, <https://www.acainternational.org/news/fcc-removes-voice-service-providers-from-robocall-mitigation-database/>