

Robocall Mitigation Policy

Business Information

E-Control Systems, Inc.
15301 Ventura Blvd
Suite D320
Sherman Oaks, CA 91403

Contact Information

Eran Bernstein
CEO
(818) 783-5229
eran.bernstein@econtrolsystems.com

1. Overview

This Robocall Mitigation Policy outlines the measures and procedures established by E-Control Systems, Inc. ("ECS") to address the growing concerns related to robocalls and ensure the integrity of the ECS communication systems. In the Commission's recent release, *In the Matter of Cal Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (released March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that an RMP include:

- "Know Your Customer" procedures.
- "Know Your Upstream Provider."
- A description of any call analytics system used to identify and block traffic.
- Whether a third-party vendor is used and if so, the name of the vendor.

2. Purpose

The purpose of this Robocall Mitigation Policy is to establish guidelines and procedures to prevent, detect, and mitigate the impact of robocalls on E-Control Systems ("ECS") organization's communication systems and the individuals associated with our services.

3. Scope

This policy applies to all employees, contractors, customers, and third-party service providers who have access to the ECS communication systems.

4. Definition of Robocalls

For the purpose of this policy, robocalls are defined as pre-recorded voice messages delivered through an automated dialing system, with the intent to promote products, services, or engage in fraudulent activities.

5. Compliance with Regulations

ECS is committed to complying with all relevant regulations and laws pertaining to robocalls, including but not limited to the Telephone Consumer Protection Act (TCPA) and the Truth in Caller ID Act.

6. Implementation of Call Authentication Technologies

ECS, in collaboration with our upstream provider, will implement and actively support call authentication technologies such as STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using toKENs). Authentication procedures will be applied at the upstream provider level to ensure the integrity of calls reaching our external communication systems.

7. User Education and Awareness

Employees and users of our communication systems will be educated about the risks of robocalls, how to identify them, and the procedures for reporting any suspicious calls. Regular awareness campaigns will be conducted.

8. Know Your Customer (KYC) Procedures

Before engaging in any communication, our organization will implement and follow robust KYC procedures to verify the identity of customers. This includes obtaining relevant identification documents, validating customer information, and conducting risk assessments. Each customer is identified using the following:

- Unique personal identification number.
- Username and password.
- Optional telephone number based identification.

9. Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eight Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in GC Docket 17-59 (Rel. May 19, 2023) Paragraphs 49-51*, ECS provides the following information concerning its upstream voice service carriers.

ECS has one upstream provider from which it sends voice traffic:

Bandwidth Inc.
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
voicesecurity@bandwidth.com

ECS has an agreement with its upstream providers and has received assurances in writing from their officials that they have, and will continue to, sign calls transmitted from/to ECS, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to ECS. ECS and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

10. Compliance with Traceback Requests

ECS will fully comply with traceback requests from authorized entities, including government agencies and telecommunication regulatory bodies. We will provide necessary information and support to trace the origin of robocalls and assist in enforcement actions.

11. Acceptable Use Policy

- **Authorized Use:** All employees, contractors, customers, and third-party service providers are authorized to use our communication systems for business purposes only. Any use of the system for personal or unauthorized activities is strictly prohibited.
- **Prohibited Activities:** The following activities are strictly prohibited:
 - Engaging in any form of robocalling or spamming.
 - Using the communication systems for illegal or fraudulent purposes.
 - Attempting to bypass or manipulate call filtering and blocking technologies.
 - Unauthorized access to communication system settings or data.
- **Data Privacy:** Users must respect the privacy of individuals associated with our services. Unauthorized access, disclosure, or sharing of sensitive information is strictly prohibited.
- **Security Measures:** Users are required to adhere to all security measures implemented by the organization, including but not limited to password policies, two-factor authentication, and encryption protocols.

12. Mitigation Through Contract

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with us).

13. During Service

All subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting).

14. Monitor Traffic with Analytics

ECS originating voice calls are automated through our internal proprietary system. Customers are not allowed to create manual calls. As such, there is little potential for fraudulent calls made through the ECS automated system. Our upstream provider, Bandwidth, has implemented a proprietary reporting process through which ECS can analyze high-volume network traffic to evaluate compliance with a variety of fraud detection indicators and fraud detection best practices.

ECS may take remedial action against any customer's account to prevent or remediate robocalling or other fraudulent activity. No other third parties are involved in deploying ECS's analytics.

15. Investigate Suspicious Activity

In the event of suspected robocall or fraudulent activity, our risk prevention team is alerted which follows the defined procedures on investigating such customer. This includes:

- Collection of relevant data and call records.
- Analysis of call patterns and anomalies.
- Cooperation with law enforcement and regulatory agencies.
- Collaboration with our upstream provider to identify and mitigate threats.

16. Reporting and Response Procedures

Any employee or user who observes or suspects suspicious activity must report it promptly to the designated risk prevention team. ECS will have established response procedures to investigate and mitigate reported incidents.

17. Regular Audits and Assessments

Regular audits and assessments of communication systems will be conducted to identify vulnerabilities and ensure the effectiveness of implemented mitigation measures, including KYC procedures and compliance with the Acceptable Use Policy. Any weaknesses or gaps will be addressed promptly.

18. Disciplinary Action

Any employee found in violation of this policy will be subject to disciplinary action, which may include but is not limited to warnings, suspension, or termination, depending on the severity and recurrence of the violation.

19. Review and Updates

This Robocall Mitigation Policy and the Acceptable Use Policy will be reviewed periodically to ensure their relevance and effectiveness. Updates will be made as necessary to address emerging threats,

technological advancements, changes in regulations, and to maintain the integrity of our communication systems.

20. Communication of the Policy

This policy, including the Acceptable Use Policy, will be communicated to all employees, contractors, customers, and third-party service providers through training sessions, email communications, and inclusion in relevant documentation.

21. Principles, Affiliates, Subsidiaries, and Parent Companies

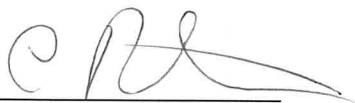
Eran Bernstein, Adam Campbell, and Abraham Bernstein are the principals of E-Control Systems, Inc. Eran Bernstein and Adam Campbell are Co-CEOs and Abraham Bernstein is Chairman of the Board. They own 100% of the shares in E-Control Systems. Below are the parent and/or subsidiaries and affiliates of E-Control Systems, Inc.:

FILING ENTITY: E-Control Systems, Inc.			
<u>Legal Name</u>	<u>Relationship to Filing Entity</u>	<u>Percentage Owned by Filing Entity</u>	<u>Management/Control of Entity</u>
E-Control Systems, Inc.	Self/Filing Entity	100%	Eran Bernstein Adam Campbell Abraham Bernstein
E-Control Systems (India) Private Limited	Subsidiary (Engineering Entity)	100%	Eran Bernstein

Certification of Eran Bernstein

I, Eran Bernstein, CEO of E-Control Systems, Inc. ("ECS") do hereby certify, under penalty of perjury, the following:

- a. ECS is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure. To the best of our knowledge, and consistent with the upstream partners RMP, upstream partner has fully implemented STIR/SHAKEN controls.
- b. ECS's business name and primary address is as follows:
E-Control Systems, Inc.
15301 Ventura Blvd.
Suite D320
Sherman Oaks, CA 91403
- c. ECS has no other business names in use for the voice services referenced.
- d. ECS has not previously used any other business name for the voice services referenced.
- e. The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- f. ECS's role in the call chain is that of a voice service provider with no STIR/SHAKEN implementation obligations.
- g. ECS is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- h. ECS has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- i. ECS is not required to, and does not have, an Operator Code Number



Eran Bernstein