

Robocall Mitigation Plan
Hybrid IT Services, Inc.
FRN # 0031543903
RMD0009094

Effective Date: Dec 1st 2024

Purpose:

Hybrid IT Services, Inc. is committed to complying with all applicable laws and regulations to mitigate robocall traffic and ensure the responsible use of Voice over Internet Protocol (VoIP) services. This Robocall Mitigation Plan outlines the steps and policies in place to prevent robocalls and unauthorized use of telephony systems.

1. Scope and Applicability

This Robocall Mitigation Plan applies to:

- All internal VoIP usage by Hybrid IT Services, Inc.
- Users of Hybrid IT Services' proprietary software product, **Chat Roster**.

2. Internal VoIP Usage

Hybrid IT Services, Inc. uses VoIP services exclusively for **manual calls** by its employees. The company:

- **Does not and will not use robocall services.**
- **Prohibits SIP trunking** or any automated dialing mechanisms within its internal operations.

All employees are required to adhere to this policy and report any potential misuse immediately.

3. Chat Roster Customer Policies

Hybrid IT Services, Inc. mandates that all users of its software product, **Chat Roster**, agree to the following terms regarding VoIP and telephony usage:

1. Prohibition of Robocalls:

- Customers must not use Chat Roster or any associated telephony features to initiate robocalls or automated dialing.

2. No SIP Trunking:

- Chat Roster does not support SIP trunking, nor does it allow customers to integrate VoIP services for automated dialing purposes.

3. Compliance Agreement:

- Customers must sign an agreement to abide by Hybrid IT Services' Robocall Mitigation Plan and applicable regulations, ensuring their usage complies with these standards.

Acceptable Use – Terms & Conditions for Users

Hybrid IT Service, Inc maintains a zero tolerance policy for SMS Spam, Mobile Spam, Text Messaging Spam. You are solely responsible for any activity that occurs under your user names and accounts. You expressly agree that you will not resell the Service, Service Data, and/or Mobile App. You may not assign your obligations under these Terms to any other party. We are not liable to you for any unauthorized access to or misuse of the Service, Service Data, and/or

Mobile App. You may not use the Service, Service Data, and/or Mobile App in any manner that could damage, disable, overburden, or impair the Site or interfere with any other party's use and enjoyment of the Site. You may not attempt to gain unauthorized access to the Site (or computer systems or networks connected to the Service, Service Data and/or Mobile App) through hacking, password mining, or any other means. You agree that you will not engage in any activities with respect to the Service, Service Data, and/or Mobile App that violate any applicable local, state, national or international laws or regulations, the intellectual property or other rights of third parties, or submit or transmit any material that is abusive, defamatory, obscene, threatening, or otherwise inappropriate, as reasonably determined by the Company. You are required to use the Services in full compliance with all applicable laws and regulations, including without limitation, all state, federal and international: (a) Do-Not-Call ("DNC") list prohibitions; (b) telemarketer licensing and bonding requirements; (c) consumer cancellation rights; (d) mandatory disclosures; (e) wireless calling restrictions; (f) restrictions on the use of automatic telephone dialing systems and pre-recorded messages (i.e. robocalling or voice broadcasting); (g) internal opt-out rules; (h) intellectual property rights and restrictions; and (i) other product and industry specific rules and disclosures. By making any use of the Service, Service Data, and/or Mobile App you expressly warrant to us that You are and shall continue to act in full compliance with the law. All of our offers are void where prohibited by law. You agree that You have read and understand the FTC's Telemarketing Sales Rule ("TSR") and the FCC's Telephone Consumer Protection Act ("TCPA"), and all other applicable laws and regulations. You must review these rules with your own legal counsel to ensure that you understand and are fully compliant. We do not assume responsibility for ensuring that your marketing campaigns meet applicable legal requirements. We will not assume any liability if You are ever held guilty or liable for any law violation. Notwithstanding the foregoing, you acknowledge that we have and are taking active steps to ensure the compliance of our customers, including by having you agree to these terms and otherwise.

If we discover evidence demonstrating that you may have violated the law, we may suspend or terminate your use of the Services immediately. You realize and agree that we may be required by law to provide certain information about you if we receive a subpoena from a court or regulator with competent jurisdiction. We are under no obligation to object to the same, except in our sole discretion.

Customer Vetting

- Project Broadcast collects first name, last name, email, contact phone, contact address, and IP address for all registrations. This data is used for brand and campaign registration with The Campaign Registry, and for law enforcement and traceback requests.
- Project Broadcast users select a single phone number when signing up that is tied directly to their account. They have no way to spoof their number as the platform will automatically set the caller id based as the phone number on their account when outbound calls are placed.

Outbound Call Confirmation

- When placing an outbound call the system first calls the user's cell phone and asks them

to confirm by pressing 1 in order to make the outbound call. This drastically reduces the potential for robocalling because failure to press 1 will result in call termination.

Traceback and Law Enforcement Cooperation

- Hybrid IT Service responds promptly to traceback requests from its vendors as well as the industry Traceback Group and its members. After determining the validity of such requests using platform data and logs, we follow best practices to promptly support the investigation and take appropriate action, including account suspension, termination, blocking, etc.

4. Monitoring and Enforcement

- Hybrid IT Services, Inc. will implement systems to monitor and detect unauthorized or automated robocall activities.
- Any violation of this plan by employees or customers will result in immediate action, including:
 - Revocation of software access for customers.
 - Disciplinary action for employees, up to and including termination.

5. Certification

Hybrid IT Services, Inc. certifies that it adheres to FCC guidelines and other applicable standards to mitigate robocall traffic. This certification applies both to internal operations and to the policies enforced through Chat Roster.

6. Contact Information

For questions or concerns regarding this Robocall Mitigation Plan, please contact:

Compliance Department

Hybrid IT Services, Inc.
6035 S Marin Ct
Gilbert, AZ 85298

Email: voip@hybriditservices.com
Phone: 480 307 7328

Acknowledgment

Hybrid IT Services, Inc. reaffirms its commitment to ethical telecommunication practices and the mitigation of unlawful robocall activities. This plan will be reviewed periodically and updated as necessary to ensure compliance with evolving regulations.

Approved By:

Ahmed Chishti
President, CEO

Hybrid IT Services, Inc.