



ROBOCALL MITIGATION PROGRAM

Crosswind Cloud Solutions

Jordan Morris

Contents

Robocall Mitigation Program Introduction	2
Company Summary.....	2
Robocall Mitigation Program.....	2
Knowing Your Customer and Upstream Providers.....	2
Requiring Contractual Provision to Mitigate Illegal Robocalls.....	2
Validating Customer’s Right to Use Telephone Numbers	3
Blocking Calls on a Do-Not-Originate List	3
Analyzing and Monitoring Network Traffic Routing Through Our Network	4
Investigating Suspicious Calling Patterns.....	4
Establishing Trust with Customers Networks	4
Additional Endpoint Security	5
Concurrent Call Limits.....	5
Responding to Commission, Law Enforcement and ITG Traceback Requests within 24 Hours	5
Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues	5
Updating Crosswind Cloud Solutions RMD Submission and RMP	6
Training	6

Robocall Mitigation Program Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following is Crosswind Cloud Solutions Robocall Mitigation Program (“RMP”) that it established to prevent unlawful robocalls from originating, terminating, or being carried or processed on its voice network.

Company Summary

Crosswind Cloud Solutions is an innovative VOIP provider focused on providing voice/hosted PBX solutions to Business customers. Providing a fully managed solution where we manage all customers’ configuration changes and system installations. Crosswind Cloud Solutions provides our customers with all the hardware phones and voice SD-WAN to all of us to manage the solution end to end.

Robocall Mitigation Program

This RMP applies to Crosswind Cloud Solutions calling platforms (which are all IP-based) and provides information on the following topics that are discussed in turn below which detail the specific reasonable steps Crosswind Cloud Solutions has taken to avoid originating, terminating, or carrying or processing illegal robocall traffic on its network.

Knowing Your Customer and Upstream Providers

Consistent with the FCC’s Caller ID Authentication Best Practices No. 16 and 47 C.F.R. § 64.1200(n)(4), Crosswind Cloud Solutions vets, among other things, “the identity of retail and resell subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.” In so doing, Crosswind Cloud Solutions takes “affirmative, effective measures to [(1)] prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic” and (2) know its upstream providers.

Requiring Contractual Provision to Mitigate Illegal Robocalls

Crosswind Cloud Solutions voice service customers are subject to robust terms and conditions that (1) obligate customers not to use Crosswind Cloud Solutions services for unlawful purposes; and (2) preserve Crosswind Cloud Solutions right to terminate customers for violations of the law. In particular, Crosswind Cloud Solutions mandates that each agreement with its customers incorporates Crosswind Cloud Solutions Acceptable Use Policy (“AUP”), which includes, among other things, a termination clause for violations of any law or regulation applicable to the customer’s use of Crosswind Cloud Solutions services or its equipment. Crosswind Cloud Solutions also retains the right to immediately suspend or terminate service without notice for violations of its AUP, which prohibits the use of Crosswind Cloud Solutions network, machines, or services in any manner that:

- violates any applicable law, regulation, treaty, or tariff, including but not limited to data privacy laws and laws restricting or prohibiting unlawful robocalls, telemarketing calls or messages, use of auto dialers.
- violates the acceptable use policies of any networks, machines, or services which are accessed through Crosswind Cloud Solutions network.
- violates the privacy of others.
- involves deceptive online marketing practices including, without limitation, practices that violate the United States Federal Trade Commission's guidelines for proper online marketing or telemarketing.
- involves the use or transmission of fraudulent traffic or fraudulent activity, including without limitation call spoofing, traffic pumping fraud, and fraudulent bot traffic.
- falsifies, manipulates, spoofs, or otherwise tampers with user identification information and/or caller identification information.
- fails to authenticate call traffic in accordance with applicable laws and regulations.
- furnishes false or incorrect data or information to Crosswind Cloud Solutions, including without limitation information provided on signup, Know-Your-Customer forms, or otherwise in response to any request by Crosswind Cloud Solutions to ascertain or verify the customer's identity and business practice; or
- impersonates or misrepresents the customer's affiliation with any person or entity.

In addition, Crosswind Cloud Solutions reserves the right to suspend or terminate service without notice, if the AUP or applicable law is violated. In such instances, Crosswind Cloud Solutions will discontinue service without notice and/or seek legal recourse to recover all costs involved in enforcement.

Validating Customer's Right to Use Telephone Numbers

Customers are not able to configure telephone numbers that are sent as outbound Caller ID. Crosswind Cloud Solutions NOC can configure the outgoing telephone numbers only from numbers that are assigned to the customer's account and are able to be configured for receiving inbound calls. Our Soft switch fabric adds a second layer of protection/validation in the event a customer manages to send a number not assigned to their account as an outbound CID number, our switch fabric will auto correct and transmit the customers primary BTN that is registered on our network.

Blocking Calls on a Do-Not-Originate List

When routing traffic as Gateway Provider, Crosswind Cloud Solutions blocks call in accordance with FCC Rule 47 C.F.R. § 64.1200(o)(1)-(4) purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan ("NANP") numbers. Crosswind Cloud Solutions has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number. When serving as a Voice Service Provider

Crosswind Cloud Solutions may, in accordance with FCC Rule 47 C.F.R. § 64.1200(k)(2), block such calls along with calls that %COMAPNY% identifies, based on reasonable analytics, as highly likely to be associated with a one-ring scam. Additionally, as stated above each customer can only transmit numbers that are assigned to their account as their outbound CID number.

Analyzing and Monitoring Network Traffic Routing Through Our Network

Upon receiving call traffic, Crosswind Cloud Solutions also analyzes and monitors the call traffic that originates, terminates, or is carried or processed on Crosswind Cloud Solutions voice network. Crosswind Cloud Solutions does not use a third-party analytics vendor(s). It is Crosswind Cloud Solutions policy to extract call traffic data on a real time basis to flag any suspicious activity. Activity is flagged as suspicious based on analysis of (a) call length and call count patterns, (b) cancel/86 reports, (c) 503 reports, (d) SIP data, and (e) other data sets based on known carrier algorithm performance.

Where suspicious activity is detected, Crosswind Cloud Solutions takes further steps to investigate the activity, including (a) in-depth review by the Crosswind Cloud Solutions engineering team to better understand the cause of the suspicious activity, (b) direct contact with the customer or carrier partner to address and mitigate the activity, (c) run reporting and closely watch the specific customer's activity to ensure the call traffic is valid, (d) investigate with the Industry Traceback Group; and/or (e) such other investigation as determined to be appropriate in Crosswind Cloud Solutions discretion.

Investigating Suspicious Calling Patterns

When analyzing and monitoring call traffic, if Crosswind Cloud Solutions discovers call patterns that are consistent with illegal robocalling, Crosswind Cloud Solutions, after further investigation, takes appropriate action to address such behaviors. Depending on the severity of the conduct and the information/explanation provided by the customer, corrective measures may include (a) suspension, (b) termination, (c) warnings to the customer and efforts to bring the customer within the terms of the governing contract terms and AUP, (d) throttling traffic, (e) reporting the customer to authorities, where call traffic is confirmed as illegal and potentially damaging to consumers, (f) additional monitoring, and/or (g) such other actions as deemed appropriate in the discretion of Crosswind Cloud Solutions, and consistent with law, regulations, and the governing contract(s) and Crosswind Cloud Solutions AUP.

Establishing Trust with Customers Networks

Crosswind Cloud Solutions has put in place the use of IP layer whitelists to accept traffic from a given users network or endpoint device (Physical IP phone or Softphone). If the source IP of the voice traffic is not in our approved whitelist the traffic is blocked and not able to register and thus establish a call path. We also make use of other analytics to ensure that only devices approved are granted access to the Crosswind Cloud Solutions voice network. Customers are NEVER given access to endpoints SIP credentials. This information is delivered directly to the phones/endpoints as part of the auto provisioning service for the types of endpoint hardware approved by Crosswind Cloud Solutions. Additionally, we provide customers with a CLEARity SD-WAN voice firewall that further allows us to mitigate illegal traffic before it even hits our network.

Additional Endpoint Security

We make use of different kinds of signature real time analytics to auto block devices that do not match our known trusted device signatures. When a device/endpoint is auto blocked its source IP is added to a “Do not Accept Traffic List”. The source IP can only be removed once it has been manually investigated by a member of Crosswind Cloud Solutions NOC.

Concurrent Call Limits

Each user endpoint device is limited to 4 concurrent calls. Only Crosswind Cloud Solutions NOC can increase this value based on a well-articulated need given by the end user.

Responding to Commission, Law Enforcement and ITG Traceback Requests within 24 Hours

Crosswind Cloud Solutions is committed to ensuring that its network is not utilized for the origination, termination, or carrying or processing of unwanted and illegal robocalls. In accordance with the FCC’s regulations 47 C.F.R. § 64.1200(n)(1) along with 47 C.F.R. § 64.6305(a)(2), (c)(2), (d)(2)(iii), (e)(2)(iii), and (f)(2)(iii), Crosswind Cloud Solutions will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium (“ITG”) within 24 hours and will cooperate with such entities in investigating and stopping any illegal rob callers that attempt to use Crosswind Cloud Solutions network and services to originate, carry or process calls. Crosswind Cloud Solutions will take the steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules.

Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Crosswind Cloud Solutions network is not utilized for the origination, termination, carrying, processing, or routing of unwanted and illegal robocalls, Crosswind Cloud Solutions provides the following name, title, business address, telephone number, and email address of the individual within Crosswind Cloud Solutions that leads Crosswind Cloud Solutions team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: Jordan Morris

Contact Title: VP of Development

Contact Business Address: 2201 N Camino Principal #125

Contact City: Tucson

Contact State and Zip Code: Arizona, 85715

Contact Telephone Number: 520-325-2603

Contact Email: jmorris@crosswindovip.com

Updating Crosswind Cloud Solutions RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), Crosswind Cloud Solutions will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

Training

Finally, Crosswind Cloud Solutions has implemented a training program that focuses on ensuring that personnel receive appropriate training on issues related to illegal robocalls. It is Crosswind Cloud Solutions policy that all management-level employees maintain a robust continuing education program to assure they are up to date on (a) the Company's RMP along with the associated policies and procedures that implement the RMP, and (b) latest key developments and emerging trends involving: (1) scam and fraudulent traffic and patterns to look out for, (2) regulatory requirements on carriers and carrier partners, (3) robocall mitigation efforts, (4) law enforcement and legal activity related to domestic and international calling practices, (5) legal efforts, authorizations or requirements to identify, monitor, block or limit certain calls, (6) industry concerns regarding call monitoring, blocking, labeling, and/or reporting; (7) call identification and authentication protocols and requirements; and (8) the broader legal framework applicable to Crosswind Cloud Solutions operations. Crosswind Cloud Solutions treats this continuing legal education as a critical piece of its role in the telecommunications ecosystem and its strategic position as a partner in mitigating illegal traffic.