

COGECO US FINANCE, LLC, D/B/A BREEZELINE & AFFILIATES

Robocall Mitigation Plan

September 2025 Version

Table of Contents

I.	Robocall Mitigation Program Introduction.....	3
II.	Robocall Mitigation Program	3
	1. Implementing Know-Your-Customer Protocols	3
	2. Requiring Contractual Provisions to Mitigate Illegal Robocalls	4
	3. Only Accepting Traffic from Providers in the RMD/ Know-Your-Upstream Provider Protocols.....	4
	4. Blocking Calls on a Do-Not-Originate List	4
	5. Analyzing and Monitoring Network Traffic - Call Analytics	4
	6. Responding to Commission, Law Enforcement and ITG Traceback Requests	6
	7. Designating an Employee Responsible for Addressing Robocall Mitigation- Related Issues.....	6
	8. Updating Breezeline’s RMD Submission and RMP	6

I. Robocall Mitigation Plan Introduction

This Robocall Mitigation Plan (“RMP”) applies to Cogeco US Finance, LLC d/b/a Breezeline and its Affiliates listed in Exhibit A (together, “Breezeline”), which offer interconnected VoIP services on a resold basis using the services of IDT Telecom, Inc. (“IDT”) and commercial mobile radio service (“CMRS”) on a resold basis using the services of AT&T Mobility LLC (“AT&T”). Breezeline is the eighth-largest cable operator in the United States and provides services in 13 states: Connecticut, Delaware, Florida, Maine, Maryland, Massachusetts, New Hampshire, New York, Ohio, Pennsylvania, South Carolina, Virginia and West Virginia.

While Breezeline necessarily relies on the robocall mitigation policies, procedures, and safeguards implemented by its wholesale service providers, Breezeline and its affiliates have adopted the following RMP to attempt to prevent unlawful robocalls from originating from its end user customers.

II. Robocall Mitigation Plan

This RMP describes Breezeline’s policies and procedures to engage to attempt to avoid carrying or processing illegal robocall traffic:

- (1) Implementing Know-Your-Customer Protocols
- (2) Contractual Provisions to Mitigate Illegal Robocalls
- (3) Only Accepting Traffic from Providers in the RMD/ Know-Your-Upstream Provider Protocols
- (4) Blocking Calls on a Do-Not-Originate List
- (5) Analyzing and Monitoring Network Traffic Routing Through Breezeline’s Network
- (6) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (7) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (8) Updating Breezeline’s RMD Submission and RMP

1. Implementing Know-Your-Customer Protocols

Breezeline vets the identity of potential 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, Breezeline takes affirmative, effective measures to 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.

In this regard, Breezeline has implemented appropriate Know-Your-Customer (“KYC”) protocols when onboarding new or renewing customers. As part of its KYC protocols,

Breezeline generally requires its customers to provide the full legal name and contact information, and, for commercial customers, state or country of incorporation and nature of the customer's business. Breezeline's VoIP services are provided to fixed locations using its own broadband network and services are typically installed on location by its personnel, so it knows the actual location of its customers. This information enables Breezeline to validate the identity of potential customers prior to provisioning of service. Breezeline will not provide voice service if a new customer's identification cannot be verified.

2. Contractual Provisions to Mitigate Illegal Robocalls

Breezeline's terms of service prohibit the use of Breezeline's services for unlawful purposes or in a manner that is inconsistent with normal call patterns, and enable Breezeline immediately to suspend or terminate service used in violation of these terms.

3. Only Accepting Traffic from Providers in the RMD/Know Your Upstream Provider

Breezeline's upstream providers are well-known, reputable wholesale service providers that are registered in the FCC's Robocall Mitigation Database. Breezeline does not itself have knowledge or insight into upstream providers from which its wholesale providers receive traffic, but understands from their mitigation plans that their direct upstream connections are with service providers that similarly have represented to the FCC that they have policies and procedures to identify and block unlawful robocall traffic.

4. Blocking Calls on a Do-Not-Originate List

IDT's robocall mitigation plan on file with the FCC reports that it blocks calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan numbers, and that it has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number.

AT&T's robocall mitigation plan on file with the FCC reports that it has a robocall detection process in identifying suspect calls by leveraging a broad set of data from internal proprietary as well as public sources. AT&T also reports it uses aggregation of data, which includes, but is not limited to: average call duration, call completion rates, calling identification name, call volumes and the timeframes in which calls are placed, sequential dialing patterns, complaint data, and call volumes to telephone numbers on the DNO.

5. Analyzing and Monitoring Network Traffic - Call Analytics Used to Detect and Block Unlawful Robocalls

As a reseller of interconnected VoIP services, Breezeline necessarily relies on its wholesale provider IDT to monitor and detect patterns indicative of potential unlawful robocalls and to block such calls. IDT's robocall mitigation plan reports that it:

- has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, atypical call activity, and subscriber information), receive automatic alerts, investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis;
- uses internally developed electronic as well as manual customer analytics tools designed to monitor traffic for suspicious patterns (IDT describes that what makes a pattern “suspicious” is the result of multiple factors, which may (and likely will) vary based on numerous considerations including, but not limited to: commercial history with IDT of entity transmitting traffic to IDT Telecom; terminating location of traffic; length of calls; originating ANIs of traffic; prior understanding of IDT Telecom regarding the traffic to be transported; country/region of originating calls; as well as other factors which may or may not be considered in all instances);
- uses You Mail Protective Services and compares ANIs against a Do Not Originate list provided by Somos, Inc. through their subsidiary, XConnect, to block such traffic automatically; and
- blocks all numbers on the Industry Traceback Group Do Not Origin List and is consistently reviewing and considering the implementation of additional DNO lists.

As a reseller of CMRS, Breezeline necessarily relies on its wholesale provider AT&T to monitor and detect patterns indicative of potential unlawful robocalls and to block such calls. AT&T’s mitigation plan reports that:

- AT&T’s internal data analytics and fraud teams are constantly looking for new patterns that are indicate of illegal robocalls and other ways to improve the robocall detection process;
- These teams regularly meet to share new findings and consider potential modifications to the process;
- AT&T’s fraud team detects a pattern indicative of illegal robocalling, or otherwise has reason to suspect its direct customer is engaging in illegal robocalling or spoofing, the AT&T fraud team will contact the account manager for that customer and the customer may be called to gather additional information about the business and whether it is engaged in illegal robocalling or spoofing and if AT&T determines that a customer is engaged in illegal robocalling or spoofing, AT&T’s agreements allow it to terminate or restrict that customer’s services and if AT&T’s fraud team has reasons to believe AT&T is receiving traffic from an international or domestic carrier that includes illegal robocalling or spoofing, AT&T carrier relations manager will contact the carrier and then AT&T will take appropriate action, which may include blocking traffic; and

- AT&T's fraud team utilizes a vendor, Hiya, for the analytics used in AT&T ActiveArmor for call blocking and labeling for its wireless customers on an opt-out basis at no charge and that ActiveArmor automatically blocks suspected fraud calls and labels calls that are identified as a spam risk.

If Breezeline receives a report from IDT or AT&T of suspected unlawful robocall traffic originated by its end user customer, Breezeline will conduct an investigation. To the extent a customer is found to have violated its terms of service, takes appropriate action to address such behaviors, which may include terminating the customer's service.

6. Responding to Commission, Law Enforcement and ITG Traceback Requests

Breezeline 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 robocallers that attempt to use Breezeline's network to carry or process calls. Breezeline is also committed to cooperating with its wholesale providers regarding any traceback requests that are associated with Breezeline's end user customers. As part of these commitments, Breezeline will take the necessary 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.

7. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

Breezeline provides the following name, title, department, business address, telephone number, and email address of the individual within Breezeline for inquiries regarding robocall mitigation-related issues and traceback inquiries from the FCC, ITG, and law enforcement agencies:

Sean Brushett
Chief Operations Officer
3 Batterymarch Park
Suite 200
Quincy, MA 02169
617-237-6283
legal@breezeline.com

8. Updating Breezeline's RMD Submission and RMP

Consistent with 47 C.F.R. § 64.6305(c)(5) and (d)(5), Breezeline will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.

Exhibit A

Company Name or Trade Name	<u>FRN</u>
Cogeco US Finance, LLC	0015336449
Cogeco US (CT), LLC	0024858300
Cogeco US (Delmar), LLC	0009596875
Cogeco US (Miami), LLC	0009596826
Cogeco US (NH-ME), LLC	0026868935
Cogeco US (Penn), LLC	0009596883
Cogeco US (OH), LLC	0031132186
Cogeco US (SC), LLC	0015336464