



Robocall Mitigation Plan

Contents

Company.....	3
Thorough Vetting Process.....	4
Tools and Consistent Monitoring.....	4
Know Your Upstream Providers.....	5
Modus operandi in case of illegal traffic.....	6
Commitment.....	6

Company

Business Information

- **Legal name:** Media Boil LLC
- **Business name (DBA):** Call Ocean
- **Address:** 580 Herndon Pkwy #105 Herndon VA 20170

Contact Information for Robocall Mitigation-related Issues

- **Full Name:** Christopher Michael Goetz
- **Title:** VoIP Consultant
- **Department:** Management
- **Business Address:** 580 Herndon Pkwy #105 Herndon VA 20170
- **Telephone Number:** 855.505.5855
- **Email Address:** admin@callocean.com or app@callocean.com for any law enforcement requests.

About

Call Ocean is a Virginia-based VoIP provider founded in 2015. Its customer base consists of small to medium-sized business customers. Call Ocean is a pioneer in the industry when it comes to combating illegitimate traffic (including, but not limited to, robocalls) and educating customers on this serious matter. Call Ocean is consistently working to improve its network and security standards. It strives to halt illegitimate calls across its subscribers.

The government-registered directors are Christopher Michael Goetz and Alper Sakarya.

Please note that Call Ocean has **not** been prohibited from filing in the Robocall Mitigation Database due to an enforcement action, and Call Ocean is **not** subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

Thorough Vetting Process

Before becoming a Call Ocean customer, a thorough vetting process is in place. Call Ocean is committed to continually enhancing this vetting process.

- Call Ocean is a self-serve cloud phone system. Customers can not sign up on their own without our customer support manually activating their accounts. They are **required** to undergo a Know Your Customer process, which involves providing their company name, complete physical location (including, but not limited to, street address, state, and country), phone number, email address, and the name of the contact person. If it is a business, more specifications are required,

including (number of employees, number of DID numbers owned, etc.). All this data is retained for security and law enforcement cooperation purposes, should it be deemed necessary in the future. Moreover, every customer who signs up and logs in with Call Ocean thereafter undergoes a digital fingerprinting process to ensure security and identity verification.

- When signing up, customers are also required to accept Call Ocean [Terms of Service](#) & [Privacy Policy](#). The terms include, but are not limited to, the following:
 - If the customer will be using Call Ocean for telemarketing purposes, they are not allowed on our platform. The Ocean staff analyzes each business customer on a case-by-case basis.
 - The customer agrees to set a valid Caller ID/ANI Identification.
 - Our customers agree to collaborate with law enforcement entities for any traceback requests.
 - Call Ocean reserves the right to suspend users without notice at its sole discretion if they fail to comply with its Terms of Service (including, but not limited to, immediate service termination for users engaging in or facilitating illegal activity).
- Before completing the sign-up process, customers must pass through Call Ocean's security algorithms to activate their account. While the various algorithms are highly confidential, as soon as Call Ocean detects a potential risk to its business, it will request proof of identification (e.g., a government-issued identification that matches the sign-up address). Call Ocean also utilizes third-party vendors to enhance the complexity of its algorithms. Moreover, Call Ocean automatically channels customers from high-risk areas to those who have undergone an extensive Know Your Customer process. High-risk areas are identified based on our accumulated experience, the trends we've observed over the years, and the insights provided by our downstream providers from their respective observations.

Tools and Consistent Monitoring

When a customer has been internally vetted, she/he now have access to the Call Ocean platform. Nonetheless, it remains under scrutiny by the various algorithms in place. Increased scrutiny is obviously more present for newer accounts. They also have access to **fewer resources**, such as limited outbound calling paths.

Call Ocean has several algorithms that trigger real-time alerts and notifications. A 24/7 fraud team and on-duty network team constantly monitor those above.

Customers pass their own valid Caller ID automatically when placing an outgoing call. Everything must be set up in the Call Ocean platform beforehand. Our customers are not able to make calls or send messages from a phone number that they do not own.

We took this initiative to add an extra layer of complexity to fraud and robocall mitigation. We will slowly build up this internal list.

Know Your Upstream Providers

Call Ocean makes use of a selected number of carriers to route calls in the United States, including:

- VoIP.MS
- Twilio

Call Ocean has received assurances from these providers that they will comply with the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic.

Modus operandi in case of illegal traffic

A real-time block system is activated as soon as abnormal activities are detected (including, but not limited to, abnormal spikes in calls, unusual trends, low call completion rates, systematic calling, and an excessive number of calls). Call Ocean system blocks suspicious traffic and automatically reaches out to customers to understand the highlighted behaviour. A dedicated team is always ready to follow up with the customer. Call Ocean has a zero-tolerance policy regarding potential fraud, scams, and robocall activities. Call Ocean also regularly reviews outbound call logs and analytics to monitor for any possible abuse. Finally, Call Ocean also works with its upstream providers to identify behaviors that indicate illegal call activity.

Commitment

To the extent that Call Ocean receives information from law enforcement, traceback entities, or other sources indicating that a customer is engaged in illegal robocalling, our policy is to cooperate fully, including providing the identity of any suspected illegal robocaller, in response to a legal service or process. Our internal policy is to reply to those requests within 24 hours.

In fact, Call Ocean offers a single point of contact for any law enforcement requests law.enforcement@callocean.com. Law enforcement agencies can simply provide the following information, and the request will be treated on a highly accelerated basis:

- Full name, Authorized Agency / Department,
- Phone Number,
- Nature of Request (Subscriber info, Call detail records, Billing info, etc.),
- Target Telephone Number(s),
- Request Start Date and End Date,
- Copy of the Subpoena, Court Order, Search Warrant, or Other Formal Legal Process, and
- Additional Notes (incl. specific circumstances and/or deadlines).

If there are multiple requests, we request that to submit only one legal process per email to ensure proper treatment.

While Call Ocean already had everything in place to combat illegitimate traffic (including, but not limited to, robocalls), it also fully commits to ensuring compliance with this program and continually enhancing it. Call Ocean also fully complies and is in the process of STIR-SHAKEN. In the event of any material change to this plan, Call Ocean will republish it to employees, consultants, and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.
