



Robocall Mitigation Plan

Contents

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

Company

Business Information

- **Legal name:** 9171-5573 Québec Inc.
- **Business name (DBA):** VoIP.ms
- **Address:** 200-2480, boul. des Entreprises, Terrebonne, QC, Canada, J6X 4J8

Contact Information for Robocall Mitigation-related Issues

- **Full Name:** David Rouleau
- **Title:** Chief Executive Officer
- **Department:** Management
- **Business Address:** 200-2480, boul. des Entreprises, Terrebonne, QC, Canada, J6X 4J8
- **Telephone Number:** 844.886.4767
- **Email Address:** drouleau@voip.ms or law.enforcement@voip.ms for any law enforcement requests.

About

VoIP.ms is a Montreal-based VoIP provider founded in 2007. While the great majority of its customers are Canada-based, it offers services in 100+ countries. Its customer base is made of residential customers, small-to-medium business customers and resellers. VoIP.ms is a pioneer in the industry when it comes to fighting illegitimate traffic (including but not limited to robocalls) and educating customers on this serious matter. VoIP.ms is consistently working to improve its network and security standards. It strives to halt illegitimate calls across its network.

9171-5573 Québec Inc. has also previously trademarked the name of Swiftvox in United States, Canada, and some other countries, but hasn't commercialized the name.

9171-5573 Québec Inc. is owned by:

- 9531-9422 Québec inc., and
- Fondation, le Fonds de développement de la Confédération des syndicats nationaux pour la coopération et l'emploi)

The government-registered directors are David Rouleau, Nguyen-Khan Chau and Julien Trussart.

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

Thorough Vetting Process

Prior to being an active VoIP.ms customer, there is a thorough vetting process. VoIP.ms is committed to keeping on enhancing this vetting process.

- VoIP.ms is a self-serve cloud platform. While customers can sign up on their own, they are **required** to go through a Know Your Customer process which includes providing their company name (exemption if residential), complete physical location (including, but not limited to, street address, state, and country), phone number, email address and contact person. If it is a business or a reseller, more specifications are required including (number of employees, number of DID number(s) owned, etc.). All this data is kept for security and law enforcement cooperation purposes if deemed required in the future. Moreover, every customer signing up and logging thereafter with VoIP.ms go through to a digital fingerprinting process to ensure security and identity verification.
- When signing up, customers are also required to accept VoIP.ms [Terms of Service](#) & [Privacy Policy](#). The terms include but are not limited to the following:
 - If the customer will be using VoIP.ms for telemarketing purposes, she/he has to get the written approval from VoIP.ms beforehand. VoIP.ms staff analyzes each telemarketing customer case-by-case.
 - Customer agrees to set a valid CallerID/ANI Identification.
 - Customer (when a reseller) agrees that he will be collaborating with law enforcement entities for any traceback requests.
 - VoIP.ms can suspend users without warning to its sole discretion if it doesn't respect its Terms of Service (including, but not limited to, immediate service termination if the user carry or process illegal traffic).
- Before completing the sign-up process, customers have to pass through VoIP.ms security algorithms to get their account activated. While the various algorithms are highly confidential, as soon as VoIP.ms detects a potential risk for its business, it will ask for proof of identification (e.g. government-issued identification matching the sign-up address, utility bill, selfie, business-related documentation among other requirements depending on the account type). VoIP.ms also uses third-party vendors to add layers of complexity to its algorithms. Moreover, VoIP.ms automatically channels customers from high-risk areas to the aforementioned extensive Know Your Customer process. High-risk areas are identified based on our accumulated experience and the trends we've observed over the years, as well as the insights provided by our downstream providers from their respective observations.

Tools and Consistent Monitoring

When customer has been internally vetted, she/he now has access to VoIP.ms 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 **less resources** such as limited outbound calling paths.

VoIP.ms has several algorithms that trigger real-time alerts, notifications and systematic blocks on radical or suspicious calling activities. A 24/7 fraud team and on-duty network team always monitor the aforementioned.

Customers are required to pass a valid CallerID format when attempting to place an outgoing call. Everything has to be set in the VoIP.ms platform beforehand. Effective March 31st 2023, VoIP.ms started to slowly roll out a number verification third-party vendor. The process consist of verifying the identity of the user for CallerID purposes. During the verification process, the customer is prompted to enter his phone number then receive a code via phone call or SMS message to enter and confirm its identity. In other words, any customer who will make outbound calls with a CallerID that is not one of his phone numbers with VoIP.ms have to go through the verification process.

Throughout discussions with its upstream carriers, VoIP.ms received confirmation that its carriers (listed below) were making use at the very minimum of the Industry Traceback Group Do Not Originate list and have either started to adopt or will soon adopt additional Do Not Originate lists from third-party vendors including, but not limited to, Somos and Neustar. They also confirmed that these Do No Originate lists were applied network wide and therefore VoIP.ms could benefit from it as a direct reseller. Effective August 29th, 2023 VoIP.ms launched its own internal Do Not Originate list. We took this initiative to add an extra layer of complexity to fraud and robocall mitigation and it's being updated regularly with available information shared by the government institution.

Know Your Upstream Providers

VoIP.ms makes use of a selected number of carriers to route calls in United States, including:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

VoIP.ms has received assurances from those providers that they will abide by 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 in place as soon as abnormal activities are detected (including but not limited to abnormal spike of calls, abnormal trends, low call completion statistics, systematic calling, unusual amount of calls, etc.). VoIP.ms system blocks suspicious traffic and automatically reaches out to customers to understand the highlighted behaviour. A dedicated team is always on the trigger to follow up with the customer. VoIP.ms has a zero-tolerance policy when it comes to potential fraud, scam and robocall activities. VoIP.ms also reviews outbound call logs and analytics regularly to monitor for any possible abuse. Finally, VoIP.ms also works on a quarterly basis with its upstream providers to identify behaviors which indicate illegal call activity and patterns detected.

Commitment

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

VoIP.ms also follows the Industry Traceback Group recommended best industry practices and cooperates in traceback and trace forward investigations.

As a matter of fact, VoIP.ms offers a single point of contact for any law enforcement requests: law.enforcement@voip.ms. 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 to submit only one legal process per email to ensure proper treatment.

While VoIP.ms already had everything in place to fight illegitimate traffic (including but not limited to robocalls), it also fully commits to ensure compliance with this program and to keep on enhancing it. VoIP.ms also fully complies with STIR-SHAKEN. In the event of any material change to this plan, VoIP.ms 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.
