

Switchboard Communications Inc.
150 Plains Road East
Burlington, Ontario
Canada
L7T 2C3
Tel: 905-617-7337
FRN: 0031359854

FCC Robocall Mitigation Certification

This document certifies that all calls originating on networks provided by Switchboard Communications Inc. (“Switchboard”), a foreign voice service provider based in Ontario, Canada, are subject to a robocall mitigation program meeting the requirements laid out by the Federal Communications Commission (FCC).

Switchboard has taken the necessary steps to ensure that its mitigation strategy forces caller ID information to match the originating caller’s telephone number via our layer 4 soft switch between the termination provider and the originating caller (client), and commits to responding within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that might attempt to use services provided by Switchboard to originate such calls.

At no time in the prior two years has Switchboard been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on April 25th, 2024.

Chris Young

Switchboard Communications Inc.

Robocall Mitigation Plan

As a foreign voice service provider, Switchboard has committed itself to mitigating abuse and criminal use of its services through a comprehensive program of policies and procedures aimed at awareness, prevention, control, monitoring, and detection across all of its operations. One key element of this strategy is Switchboard's Robocall Mitigation Plan.

In order to meet its obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, Switchboard has implemented the following Robocall Mitigation Plan:

Awareness

- Terms and conditions of use include verbiage informing all clients that the use of Switchboard services for robocalling is strictly prohibited and governed by federal laws and jurisdictions.
- Switchboard employees are trained on and maintain awareness of robocalling mitigation practices and technologies, compliance requirements, and changes to regulations and industry standards.
- Documentation, policies, and procedures are regularly updated to ensure alignment with changes to regulations. Any concerns or complaints raised by third parties regarding services provided by Switchboard are handled within 24 hours of notification.
- In matters of criminal investigation, Switchboard maintains a policy of working in compliance with any investigating entities responsible for upholding laws governing telecommunications.
- All sensitive information, including credentials for access to Switchboard-managed systems, are kept confidential and managed in accordance with cybersecurity best practices with a least-privilege access policy strictly enforced.

Prevention and Control

- Switchboard exclusively sells its services to clients that are governed by our organization as a managed services provider. Our organization operates as the administrator for every client that it sells to. No additional administration is available to clients, and call network configuration is setup specifically to prevent any abuse or criminal use of systems in accordance with both Switchboard's policies and best practices and current government regulations.
- Computer Telephony Integration (CTI) is prohibited in both policy and practice on all Switchboard managed networks, preventing any robocalling at the source. The ability to leverage robocalling technology is restricted across all telephony network service provided by our organization.
- Caller ID compliance is enforced in both policy and practice by restricting customer control over the configuration of any caller ID – Switchboard exclusively controls this as an administrator setting, which only our organization can set.
- Validation of the Caller ID Identity Token is performed at the layer 4 soft switch level, which lives between our upstream provider and the customer. No access to the switch is available to the customer; the originating caller ID serves as a token which is validated against the soft switch prior to being sent outbound, preventing caller ID spoofing.
- All equipment that utilizes Switchboard's VOIP service is managed directly by Switchboard, from VOIP provisioning to the phones deployed to end users. In conjunction with the prohibiting of the use of auto dialers and robocalling devices, there is no technical capacity for clients to install these devices on our closed telecom network.

Monitoring and Detection

- CDRs are checked at regular intervals to monitor for any suspicious activity or anomalous call volume, and appropriate actions are taken to promptly restrict, investigate, and action in accordance with all relevant laws and regulations.
- Alert monitoring is configured to notify Switchboard in the event of any unexpected hardware or software added to our network. Rogue IT added to Switchboard's closed network is promptly investigated and actioned; clients in violation of Switchboard's policy are subject to having services provided by Switchboard terminated.