

29 April 2024

Federal Communications Commission
45 L Street NE
Washington, DC 20554

Dear Sir or Madam,

Re: Iristel robocall mitigation plan

1. Iristel Inc. (Iristel) hereby submits a revised robocall mitigation plan pursuant to the *Sixth Caller ID Authentication Report and Order*.
2. Iristel is a Canadian Competitive Local Exchange Carrier (CLEC) with exchanges located in all ten provinces and three territories in Canada. Iristel specializes in VoIP telephony and provides wholesale VoIP services such as SIP trunks, telephone numbers, and other related IP telephony services to resellers. A significant number of Iristel's wholesale customers are U.S.A. based telecommunications service providers that have business requirements for access to Canada's PSTN.

STIR/SHAKEN implementation progress

3. Iristel has implemented STIR/SHAKEN on its network, as mandated by the Canadian Radio-Television and Telecommunications Commission (CRTC) in *Compliance and Enforcement and Telecom Decision CRTC 2021-123, STIR/SHAKEN implementation for Internet Protocol-based voice calls* for Canadian IP-based voice traffic. Iristel is a member of the Canadian Secure Token Governance Authority (CST-GA).
4. Iristel treats calls from U.S. origin to Canadian destination, and vice versa. It also occasionally transits calls from U.S. sources to U.S. destinations that transit through Canada. These calls are signed using Iristel's STIR/SHAKEN implementation which uses a certificate issued by the CST-GA. Because there is no integration currently between the Canadian and U.S. certificate authorities, this results in calls to U.S. destinations showing an invalid certificate.
5. Iristel is currently investigating the technical feasibility of implementing U.S.-based STIR/SHAKEN for U.S. calls that transit through Iristel's Canadian network.

Reasonable Steps to Avoid Originating Illegal Robocall Traffic

6. Iristel continues to take the following steps to mitigate illegal robocall traffic:

- a. Iristel retail end-users are unable to spoof their caller-ID. Iristel's soft switch is specifically configured to reject calls from its end-users if the caller-ID is spoofed.
- b. Some Iristel enterprise users may be permitted to spoof caller-ID upon request if the use case is valid. For example, a company may wish to display its main number on all outbound calls rather than individual DID numbers. However, in general, rules similar to those for retail customers apply and customers cannot spoof their caller ID information.
- c. Iristel has implemented geofencing of its soft switch to prevent access from IP addresses that originate from certain countries that were identified by Iristel's NOC as being responsible for a large volume of illicit traffic.
- d. Iristel wholesale customers (resellers) are telecommunications service providers and are required to register with the CRTC as carriers or resellers. In this case, the onus is on them to implement STIR/SHAKEN and/or mitigate robocalls and they should register with the FCC directly if they originate IP-based voice traffic that is encompassed in paragraph (c) of § 64.6305 *Robocall mitigation and certification*. Telecommunication service providers may obtain Canadian telephone numbers from Iristel and while they must route inbound calls through Iristel's network, they are not required to route outbound calls through Iristel's network. As such, Iristel does not have the ability to verify the validity of caller ID even if the caller is using an Iristel originating number because the call may not flow through the Iristel network.
- e. Iristel cooperates with law enforcement requests regarding spoofed or fraudulent calls. In the majority of cases, when law enforcement requests customer of record information from Iristel, it relates to a number that Iristel has assigned to a reseller. In the event that the number is assigned to a reseller (as opposed to a direct Iristel end user customer), Canadian law and Iristel's commercial terms and conditions allows Iristel to provide to law enforcement the identity of the telecommunication service provider to whom the number has been assigned without a production order. Iristel responds to these law enforcement requests promptly, usually within 48 hours, by directing law enforcement to the appropriate telecommunications service provider. This removes the ability of a reseller to hide behind a carrier because it does not have its own numbering resources that can be looked up.



- f. Iristel rejects all calls that originate, transit or terminate on its network if the caller ID contains a number that is not valid under NANP or E.164, in conformance with the requirements of Compliance and Enforcement and Telecom Regulatory Policy CRTC 2018-484 *Implementation of universal network-level blocking of calls with blatantly illegitimate caller identification*.

Commitment to Respond to Traceback Requests

7. Iristel participates in the ITG's traceback process, and is one of thirteen service providers that participate voluntarily in the CRTC's Canadian traceback process. Iristel commits to responding fully and in a timely manner 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 use its service to originate calls.

Additional Information

8. Iristel's corporate address is as follows:

675 Cochrane Drive, East Tower, 6th Floor
Markham, Ontario, L3R 0B8
Tel: 416-800-4747

Iristel is affiliated with Ice Wireless, a Wireless Carrier registered with the CRTC and providing mobile wireless service in Northern Canada. Ice Wireless uses the same corporate address, above.

9. Iristel operates the following OCNs:

154E - Iristel
630G - Ice Wireless
346J - Iristel Wireless

Sincerely,

[Submitted electronically]

Jean-François Dumoulin
Regulatory Advisor



cc: Samer Bishay, Iristel CEO

*** End of Document ***