

## **Robocall Mitigation Plan**

### Business Information

Insta-Info Inc.  
866 A East Franklin Street  
Dayton, Ohio 45459

### Contact Information

Douglas Fritz  
President  
937-439-0064 x 374  
[dfritz@insta.info](mailto:dfritz@insta.info)

### Overview

In the Commission's recent release, *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (2023) ("R&O"), it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

### Purpose

Insta-Info Inc. ("Insta-Info") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Insta-Info is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Insta-Info was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Insta-Info now file RMPs. This document delineates Insta-Info's RMP. Because Insta-Info does not have access to the necessary infrastructure, it relies on its upstream carriers to assist in robocall mitigation. As delineated herein, Insta-Info works closely with its upstream providers to carry out the required mitigation functions.

### Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Insta-Info in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

All of our customers are known through a contractual agreement; we do not accept customers via web sales. Our customers are all personally known to us, and we only set up phone numbers for them to use that we purchase for them or we port in from their existing carrier. We monitor all use of our services through our own daily monitoring software. The customers are unable to set their own Caller IDs.

We know all of our customers via face-to-face meetings. We require a signed Agreement from each customer to allow them access to our services. We control the Caller ID information that our customers utilize. We will either register the telephone number for them or, if they use a phone number they own with another provider, allow the use of their existing number as part of our Agreement with them.

Insta-Info's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- physical business location;
- contact person(s);
- nature of the customer's business.

#### Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls, and Call Authentication Trust Anchor*, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404 (2023), Insta-Info provides the following information concerning its upstream voice service carriers.

Insta-Info has two upstream providers from which it receives voice traffic:

- 1) Bandwidth Inc.  
85 Allen St, Suite 310  
Rochester, NY 14608  
Gentry Williamson  
[gwilliamson@bandwidth.com](mailto:gwilliamson@bandwidth.com)
- 1) SIP.US LLC  
12725 Morris Road  
Suite 420  
Alpharetta GA 30004  
Marc Fribush  
[marc@sip.us](mailto:marc@sip.us)

Insta-Info has master service agreements with its upstream providers and has received assurances from their officials that they have, and will continue to, sign calls transmitted to Insta-Info and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Insta-Info. Insta-Info and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

### Acceptable Use Policy ("AUP")

Insta-Info's agreement template contains an AUP to which subscribers must agree in writing before being permitted to use Insta-Info's network.

For example, users agree to comply with the rules and regulations with specific regard to the Federal Trade Commission and the Federal Communications Commission National Do Not Call Registry rules and regulations and individual State Do Not Call Lists rules and regulations, along with any other similar laws that may be applicable to User's use of the Insta-Info's service. Users agree not to violate these, or any other applicable Federal or State laws, and represent and warrant that use of Insta-Info's services will not cause Insta-Info Inc. to violate these or similar laws. Users agree to comply with the anti-solicitation provisions of the Federal Telephone Consumer Protection Act of 1991, and any amendments thereto, at 47 U.S.C. § 227, the Federal Communications Commission's implementing regulations, at 47 CFR § 64.1200 et seq., and any other similar laws.

Insta-Info's contractual terms with subscribers specify that Insta-Info may take action up to suspension or termination of service for violation of the AUP.

### Analytics for Monitoring Traffic

Insta-Info works with its upstream providers to identify behaviors which indicate illegal call activity.

We maintain detailed call logs for all calls generated from our autodialer. We also maintain complete records of phone calls for all outbound autodialer calls. Finally, we can review call logs on our service providers.

Examples of calling patterns monitored are:

- anomalies in cost generated by calls from a single customer;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for typical service usage).

### Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Insta-Info works with its upstream providers to follow defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

We utilize traffic analytics from our two providers, Bandwidth and SIP.us to monitor usage and .detect abuse. Because Insta-Info does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Insta-Info's analytics.

Insta-Info follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Insta-Info will devote sufficient resources to provide prompt and complete resources to traceback requests. Insta-Info commits to responding to traceback requests fully within 24 hours.

Insta-Info works with its upstream providers to investigate suspicious activity found by the carriers' monitoring systems or reported to Insta-Info by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Insta-Info contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream providers to block their use of the platform.

For all new and renegotiated Insta-Info contracts governing the transport of voice calls, Insta-Info will endeavor to contractually require Insta-Info's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

#### Blocking

Insta-Info will implement Do Not Originate requests it receives from ITG. Insta-Info's upstream providers have mechanisms to automatically block suspicious calls using internal analytics. If Insta-Info and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Insta-Info will take appropriate action which may include suspending or terminating the subscriber's use of Insta-Info's service. Insta-Info will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto.

#### Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Insta-Info will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, Insta-Info 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.

### **Certification of Douglas Fritz**

I, Douglas Fritz, President of Insta-Info Inc. ("Insta-Info"), do hereby certify, under penalty of perjury, the following:

- (1) Insta-Info, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- (2) Insta-Info 's Business name and primary address are as follows:  
Insta-Info Inc.  
866 A East Franklin Street  
Dayton, Ohio 45459
- (3) Insta-Info uses the following d/b/a name: The Education Connection.
- (4) Insta-Info has not previously used any other business name.
- (5) Insta-Info's sole 10%+ owner and principal is Douglas Fritz. He has not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding. Insta-Info has no subsidiaries or affiliates.
- (6) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (7) Insta-Info's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (8) Insta-Info has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Insta-Info is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Insta-Info is not required to have, and does not have an operating company number.

/s/ Douglas Fritz  
Douglas Fritz

Date: December 31, 2024