

IRIS Robocall Mitigation Program

Purpose:

The primary goal of IRIS Network's RMP is to reduce the impact of illegal and fraudulent robocalls transitioning through its network via its access tandem. By working with the sub-tended ILEC companies and the IXC carriers accessing IRIS' tandem, IRIS aims to enhance the overall calling experience for its carrier's end-user customers.

Implementation Steps:

1. **STIR/SHAKEN:**
 - IRIS has not deployed a **STIR/SHAKEN** caller authentication framework to validate the identity of originating callers. This is due to two criteria: IRIS does not service end-users directly, and the tandem to our sub-tending offices is still TDM-based.
 - Our status is a non-gateway intermediary carrier; IRIS has no end-users or NPA-NXX codes. Therefore, we do not directly originate nor terminate voice calls.
 - We are still primarily a TDM tandem, as the pathways to our sub-tending end offices are TDM (e.g., DS1) based. Before a company adds SIP connections, IRIS requires they follow STIR/SHAKEN protocol in their originating traffic.
2. **Call Blocking and Filtering:**
 - Unless at the direction of the ILECs sub-tending the tandem, IRIS does not block calls transitioning through our tandem switch.
 - We collaborate with both our sub-tending ILEC carriers and IXCs that interconnect with our tandem on suspicious call activity.
3. **Traffic Analysis:**
 - IRIS periodically reviews traffic reports to review unusual activity. IRIS then consults with the sub-tended ILECs or IXC customers if it is outside of traffic pattern switching. At the request of the sub-tended ILECs or IXC customers, any suspicious traffic is investigated.
4. **Traceback Cooperation:**
 - When requested and with proper authorization, IRIS cooperates with law enforcement agencies, the FCC, and industry traceback consortia.
 - When requested, IRIS provides timely information for traceback investigations within 24 hours or other specified deadlines.
 - IRIS' commitment to assisting in stopping illegal robocalls is unwavering.
5. **Consumer Education:**
 - IRIS has limited business voice customers via 3rd-party voice platforms and does not switch end-user traffic. However, we educate carrier customers on IRIS' tandem capability.

Compliance: IRIS certifies its adherence to this RMP by filing with the **Robocall Mitigation Database** as required by the FCC. IRIS' commitment to mitigating robocalls aligns with industry practices and regulatory guidelines.

IRIS Robocall Mitigation Program

Voice Services Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that IRIS Networks has implemented to detect and prevent illegal robocalls on its network or those to be caused by its customers. IRIS Networks will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described.

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

Risk Assessment. IRIS Networks is a voice service provider offering a variety of voice calling Services via national third-party networks to selected Enterprise customers. It does not service the consumer markets. IRIS Networks does not directly switch calls, nor is it directly involved with the voice service's call processing. All customers are known to IRIS and generally do not originate high-volume calls and use other non-related IRIS Networks services. Therefore, IRIS Networks does not consider its network to be at high risk of originating illegal robocalls.

Know Your Customer: Customer Due Diligence. IRIS Networks conducts due diligence on new and renewing customers, confirming the customer's identity and publicly available business-related incorporation documents.

- IRIS Networks confirms the customer service address for all customers.
- IRIS Networks has assigned an account person to every customer.
- IRIS Networks verifies the customer's credit history and business before providing service.
- IRIS Networks verifies customer information when contracts are renewed or services are added.
- IRIS Networks verifies the customer's identity and their right to use the telephone number presented on calls.
- IRIS Networks has policies that define the circumstances by which it will deny, suspend, or terminate service to a customer.

Enforcement. If IRIS Networks has a reasonable basis to believe that a customer is originating illegal robocalls or if a pattern of questionable activity is detected, the customer will be required to remedy the problem. If the customer does not take effective action, IRIS Networks will suspend and/or terminate the customer's service.

IRIS Robocall Mitigation Program

Addendum – Specific FCC Regulation – Provides more specific guidance to the FCC’s robocall rules and our MRP.

64.6305 Robocall mitigation and certification.

(f) Certification by non-gateway intermediate providers in the Robocall Mitigation Database.

(1) A non-gateway intermediate provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with paragraph (c), that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

- (i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302(b);
- (ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302(b); or
- (iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

(2) A non-gateway intermediate provider shall include the following information in its certification made pursuant to paragraph (f)(1) in English or with a certified English translation:

- (i) Identification of the type of extension or extensions the non-gateway intermediate provider received under § 64.6304, if the non-gateway intermediate provider is not a foreign provider, and the basis for the extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;
- (ii) The specific reasonable steps the non-gateway intermediate provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of any procedures in place to know its upstream providers and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name of such vendor(s);
- (iii) A statement of the non-gateway intermediate provider’s commitment to respond 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 carry or process calls; an