



## STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Oneida County Rural Telephone ("Oneida") submits this report on its implementation of the STIR/SHAKEN call authentication framework and its program in place to prevent and mitigate illegal robocalls. This report describes the implementation of STIR/SHAKEN and the practices and procedures Oneida has in place to mitigate illegal robocalls.

### STIR/SHAKEN Implementation

Oneida has implemented STIR/SHAKEN through use of the TransNexus ClearIP. This is a managed end-to-end call authentication solution that fully satisfies the FCC's STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226 and SHAKEN – ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

Oneida implemented this solution in the IP portions of its network.

- ☒ My traffic is fully attested.
- ☐ My traffic is partially attested.
- ☐ None of my traffic is yet attested, however I have implemented the Robocall Mitigation Plan outlined below

### Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Oneida has implemented to detect and prevent illegal robocalls originated on its network. Oneida will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described.

**Risk Assessment.** Oneida is a voice service provider offering a variety of voice calling services. Its customers generally do not originate high volume calls and Oneida has not received information suggesting that robocalls are originated on its network. Therefore, Oneida does not consider its network at high risk of originating illegal robocalls.

## SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

**Customer Due Diligence:** Oneida is a long-established provider that maintains close relationships with its customers. Oneida conducts due diligence on new and renewing customers to confirm the customer's identity. Oneida confirms the customer's service address for all customers, and many transactions involve a Oneida representative visiting the customer location.

- Oneida verifies customer information when contracts are renewed, or services are added.
- Oneida verifies the customer's identity and their right to use the telephone number presented on calls.
- Oneida has the policies that define the circumstances by which it will deny, suspend or terminate service to a customer.

### **Measures to Prevent or Avoid the Origination of Illegal Robocalls**

- Oneida has in place an enforceable term of use and/or an acceptable use policy. Oneida also has in place policies designed to detect and prevent fraudulent traffic on its network.
- Oneida uses TransNexus ClearIP analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If Oneida has a reasonable basis to believe that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, Oneida can suspend and/or terminate service to the customer.
- Oneida blocks the following types of calls by default:
  - ☒ Calls originating from invalid numbers per FCC Order [2017 Call Blocking Order]
  - ☒ Calls from DNO numbers as per FCC Order [2017 Call Blocking Order]
- Oneida knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Oneida monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity, notifies the upstream carriers of any such traffic and warns the carriers that if the traffic does not cease, the calls may be blocked from entering Oneida's network. In addition, Oneida is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

### Responding to Traceback Requests

- Oneida has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. It either has provided the ITG with the contact information and business hours for those individuals or will do so upon receipt of the first request from the ITG.
- Oneida commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. Oneida commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours. If a pattern of questionable activity is detected, Oneida will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

### Cooperation with State and Federal Regulators

Oneida will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, Oneida will:

- Respond to valid law enforcement requests.
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

Oneida has deployed call authentication, call labeling, and call blocking services provided by TransNexus ClearIP. We have made great strides to protect our networks and consumers from harmful calls. Oneida is pleased to play a role in that improvement and will continue the necessary work to protect our customers.

Sincerely,

  
Heather Kirkland  
CFO