

NCC Enterprises

ROBOCALL MITIGATION PLAN

NCC Enterprises, Operating Company Number 587A, is eligible for the continuing extension of the STIR SHAKEN implementation deadline as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d).

NCC Enterprises provides local service to fewer than 100,000 voice subscriber lines. Most customers are served on the IP portions of NCC Enterprise's network which relies on technology that initiate, maintain, carry, process, and terminate SIP calls.

To meet the non-IP network criteria for the continuing STIR SHAKEN extension (§64.6303 (a)(2)), NCC Enterprises Parent Company, Northwest Communications Cooperative, is a member of NTCA. NTCA participates on the ATIS PTSC Non-IP Call Authentication Task Force working group which developed the (ATIS Solutions) non-IP call authentication solutions. NTCA is serving as NCC Enterprises third-party representative on the ATIS PTSC Non-IP Call Authentication Task Force working group.

NCC Enterprise's non-IP network is connected to carriers that have stated they do not support IP connectivity; therefore, NCC Enterprises cannot upgrade those Non-IP portions of its network to IP connectivity.

NCC Enterprise's network also has IP-portions which originates calls via SIP connections to other carriers. NCC Enterprises has registered with the Policy Administrator (via its affiliate Northwest Communications Cooperative) and is an authorized service provider in the STIR|SHAKEN ecosystem. NCC Enterprises has implemented STIR|SHAKEN within the IP portions of its network and signs the calls originating on the IP portions of its network.

Robocall Mitigation Plan

All voice traffic that originates on NCC Enterprise's network is subject to the following Robocall Mitigation Plan.

Call Analytics

NCC Enterprises has contracted with ClearIP/Toly Digital to provide robocall analytics and reputation scoring of our network's outbound traffic. ClearIP/Toly Digital uses negative reputation telephone number monitors. NCC Enterprises provides daily updates, if necessary to the ClearIP/Toly Digital database.

NCC Enterprises blocks the origination of calls from unassigned telephone numbers out of its assigned NPA-NXX inventory and calls originating from numbers that are not valid NANP numbers. Examples of such invalid numbers include those that use an unassigned area code; that use an abbreviated dialing code, such as 91155 or 411, in place of an area code; that do not contain the requisite number of digits; and that are a single digit repeated, such as 000-000-0000, with the exception of 888-888-8888, which is an assignable number.

NCC Enterprises also blocks the origination of calls from telephone numbers on its internal Do Not Originate (DNO) list. [See Appendix A](#)

Additional Traffic Monitoring & Analytics

NCC Enterprises also routes traffic via Toly Digital's networks. Toly Digital monitors all originating network traffic for suspicious or abnormal call pattern, volume or activity. NCC Enterprises is notified of any calls that meet the below qualifying factors, and the telephone numbers are investigated internally to determine if the calls are legitimate or unlawful:

- High-volume voice network traffic
- Large bursts of calls in a short timeframe
- Short duration calls
- Low average call duration
- Low call completion ratios
- Sequential dialing patterns
- Neighbor spoofing patterns

Investigation

NCC Enterprises/Toly Digital investigates calls identified as potential illegal robocalls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if NCC Enterprises/Toly Digital has any other reason to suspect illegal robocalling or spoofing is taking place over its network, NCC Enterprises/Toly Digital will work internally to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

Enforcement

Illegal robocalls and fraudulent spoofing is prohibited on our network. If it is determined an NCC Enterprises/Toly Digital customer is using our network to fraudulently spoof calls or to originate illegal robocalls, NCC Enterprises will either warn the customer to stop such practices or terminate their service as allowed per NCC Enterprises policy.

All NCC Enterprises customers receive notice of our company's prohibited use of its network for the initiation of fraudulent spoofing and robocalls. If the customer is found in violation of the prohibited use terms, their service may be terminated.

Know your Customer

NCC Enterprises has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. NCC Enterprises thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Upstream Provider Knowledge

NCC Enterprises/**Toly Digital** knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. NCC Enterprises/**Toly Digital** monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity. The connected carriers are made aware of any suspicious or illegal traffic identified and notified that, if the traffic does not cease, the calls may be blocked from entering NCC Enterprise's network. NCC Enterprises does not directly receive traffic from any foreign originating or intermediate provider. No provider is using NCC Enterprise's network to carry or process a high volume of illegal traffic. In addition, NCC Enterprises/**Toly Digital** is now incorporating traceback and prohibited traffic language in all contractual agreements with upstream carriers. [See Appendix A](#)

Traceback

NCC Enterprises 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. NCC Enterprises will respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully within twenty-four (24) hours. [See Appendix A](#)

Management and Ownership

NCC Enterprises Board of Directors

- Lorena Lambrecht – President
- Jim Simonson – Vice President
- Leslie Grubb – Secretary/Treasurer
- Roger Manger – Board Member
- Troy Donnelly – Board Member
- AJ Cvancara – Board Member
- Nate Jepsen - Board Member

Jeremy Becker serves as CEO of NCC Enterprises.

Jeremy Becker has Managing Control of NCC Enterprises and all its affiliates and subsidiaries.

NCC Enterprise is a wholly owned subsidiary of Northwest Communications Cooperative.

Appendix A

Traceback Request Single Point of Contact:

Name: Todd Watterud

Title: COO

Phone Number: 701-568-8125 or cell: 701-570-9916

Email Address: toddw@nccnd.com

Upstream Provider Information:

Name of Upstream Provider: Toly Digital

Nature of Business: Switch Provider

Network Location of Upstream Provider: Chicago, IL

Name of contact: Mark Suto

Title: Chief of Operations & Technology

Phone Number: 516-694-8655

Email Address: mark.suto@tolydigital.net

Call Analytics Vendor Name and Description of System:

Name of Vendor: Toly Digital For Robocall Mitigation

Description of the call analytics system

Call analytics purchased from the vendor determine if originating calls should be blocked. If the telephone number appears on a Do-not-call list or otherwise is an unallocated, unused, or invalid number, the call will be determined to be fraudulent and needs to be blocked. Vendor may also use advanced fraud detection which enables behavior analysis and tracking of abnormal and unexpected calling patterns to detect high volume robocalling, spoofing, and suspicious call activity.