

Vermont Data Networks, Inc. ROBOCALL MITIGATION PLAN

Vermont Data Networks (VDN), Operating Company Number 208H, 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).

VDN provides local service to fewer than 100,000 voice subscriber lines. The majority of customers are served on the non-IP portions of VDN's network which relies on technology that cannot 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)), VDN is a member of NTCA. NTCA participates on the ATIS Non-IP taskforce working group which developed the (ATIS Solutions) non-IP call authentication solutions. NTCA is serving as VDN's third party representative on the ATIS Non-IP taskforce working group.

VDN also originates calls via SIP connections within its network. Vermont Telephone Company and VDN share the same switch, VDN is the CLEC entity under Vermont Telephone Company. Vermont Telephone Company has registered with the Policy Administrator and is an authorized service provider in the STIR|SHAKEN ecosystem. Vermont Telephone Company has implemented STIR|SHAKEN within its IP-network and signs the VDN calls originating on the IP portions of VDN's network.

Robocall Mitigation Plan

All calls that originate on VDN's network are subject to the described robocall mitigation program.

Internal Traffic Monitoring & Call Analytics

VDN blocks calls originating from numbers that are not valid North American Numbering Plan (NANP) numbers, known numbers not allocated to a provider and numbers not assigned to a VDN subscriber or otherwise set aside for outbound call use.

VDN has contracted with Neustar to provide robocall analytics and reputation scoring of our network's outbound traffic. The Neustar analytics identify patterns of suspected illegal robocalls and scores the calls based on their behavior and/or their status as suspected robocalls as reported to the Federal Communications Commission (FCC), Federal Trade Commission (FTC), and as reported by other carriers. VDN has access to the Neustar's portal and receives real-time notifications about telephone numbers originating suspected illegal robocalls on its network, including from unassigned, inactive and do-not-originate TNs. VDN will also receive reports via e-mail alerts if any of its numbers experience a change in reputation such as suspicious traffic patterns or other detected anomalies outside the normal behaviour of our company's traffic. VDN will examine the reports and investigate and identify the source of the calls as unlawful or legitimate.

Investigation

VDN investigates calls identified by its analytics vendor and internal traffic monitoring as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if VDN has any other reason to suspect illegal robocalling or spoofing is taking place over its network, VDN 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 a VDN customer is using our network to fraudulently spoof calls or to originate illegal robocalls, VDN will either warn the customer to stop such practices or terminate their service as allowed per VDN policy.

Know your Customer

VDN has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. VDN 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. VDN also requires a photo ID for all new customers requesting voice service.

All new and renewing VDN customers receive notice of the VDN Terms of Service which includes notice that VDN prohibits use of its network for the initiation of fraudulent spoofing and robocalls and if end users are found in violate of the service terms, the end user's service may be terminated.

Upstream Provider Knowledge

VDN knows all the carriers from which it receives traffic and has confirmed that all its connected carriers are listed in the Robocall Mitigation Database.

VDN has also reviewed the connected carrier's RMPs to learn how the carriers monitor their originating traffic to mitigation illegal robocalls.

In addition, VDN is now incorporating traceback and prohibited traffic language in all contractual agreements with upstream carriers.

Role In the Call Chain

VDN is a voice service provider with a STIR/SHAKEN implementation obligation on the IP-Portions of its network. VDN is also a voice service provider without a STIR/SHAKEN obligation on the Non-IP portions of its network because that portion of VDN's network relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Traceback

VDN 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. VDN will respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully and in a timely manner within twenty-four (24) hours.

Robocall Mitigation Database Eligibility

VDN has not been involved in any recent, formal law enforcement or regulatory investigation into suspected unlawful robocalling.

VDN has not been prohibited from filing in the Robocall Mitigation Database (RMD).

Customer Education

VDN posts information on its website to educate customers on how to protect themselves from becoming a victim of unlawful robocalls and a process to report complaints related to robocall activity.