

**STIR/SHAKEN IMPLEMENTATION
ROBOCALL MITIGATION IMPLEMENTATION**

**Netrix, LLC
Robocall Mitigation Plan**

Background

Netrix, LLC ("Netrix" or "Company") provides a comprehensive range of services to enterprise customers, including network management, virtual desktop, cloud storage, omnichannel cloud contact center, and corporate communications solutions. Netrix provides its voice services by incorporating the resold voice over IP ("VoIP") services of Bandwidth.com, Lumen Technologies, Telnyx LLC, and IDT Telecom, Inc.

For purposes of protecting its customers from illegal robocalls and caller ID spoofing, Netrix relies on the policies, procedures and safeguards implemented by these underlying voice service providers, each of whom has fully implemented STIR/SHAKEN. Thus, all calls that the Company originates are compliant with section 64.6301(a)(1) and (2) of the Commission's rules.

Company Information

Filer's OCN: N/A

Role played in the call chain: Netrix is a voice service provider serving end-user customers via resale.

Detailed information supporting any claimed STIR/SHAKEN implementation extension or exemption: N/A

Principals, affiliates, subsidiaries, and parent companies: Netrix is a portfolio company of OceanSound Partners, LP, a private equity firm that invests in technology services companies. In this context, Netrix is wholly owned by Blue Sky Holdco, LLC which is wholly owned by OSP Lakeside Holdings 2, LLC, which is wholly owned by OSP Lakeside Intermediate Holdings, LLC which, in turn, is wholly owned by OSP Lakeside Holdings, LLC.

Other business names in use: Netrix Global (d/b/a)

All business names previously used: TetraVX (d/b/a)

Company is not a foreign voice service provider.

Persons within company responsible for addressing robocall mitigation-related issues:

- Ashish Thakkar, VP Product Development, 972-807-1988, athakkar@netrixllc.com, 2801 Lakeside Dr., Suite 125, Bannockburn, IL 60015
- David Ter Molen, General Counsel, 708-297-2636, dtermolen@netrixllc.com, 2801 Lakeside Dr., Suite 125, Bannockburn, IL 60015

Enforcement

Netrix and/or any entity for which the filing entity shares common ownership, management, directors, or control have never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program. The Company has not been prohibited by the Commission from filing in the Robocall Mitigation Database.

Robocall Mitigation

Netrix has implemented the robocall mitigation procedures set forth below. All voice traffic that originates on our network is subject to the attached Robocall Mitigation Plan. Netrix will periodically assess relevant risks and evaluate the effectiveness of its policies and procedures and may modify its procedures from time to time.

Netrix is meeting its obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls.

Know your customer, especially new customers – customer vetting:

- Netrix reviews caller ID and call records when service is installed to verify legitimate caller ID information.
- Netrix reviews new customers requesting an excessive number of call paths; screen for legitimate usage needs.

Service limitations:

- Netrix limits customers so that they can place only a limited number of calls at the same time and within a fixed time period (calls per second or CPS).
- Netrix ensures that all customers are only able to place calls originating from their own phone number either in the Caller ID field or in the diversion header / redirecting number field.

Contractual provisions. Our Terms and Conditions expressly prohibit clients from using voice services for toll fraud; unlawful autodialing or predictive dialing practices; continuous or extensive call forwarding; constant dialing; iterative dialing; fax broadcast; fax blasting; junk faxing; fax spamming; transmitting broadcasts or recorded material; sending unsolicited messages or advertisements; telemarketing; sending bulk and/ or junk email, voicemail, or faxes; taking any action to attempt to mislead others as to the identity of the sender or the origin of any communication; or any other activity that would be in violation of the Telephone Consumer Protection Act (“TCPA”) or similar state law/s or regulation/s. Our Terms and Conditions also prohibit clients from (1) re-classifying or re-originating traffic or taking any other action to intentionally make traffic appear as if it: (i) is anything other than the type of traffic delivered to such called party (including but not limited to making TDM originated traffic appear to be IP originated) or (ii) originated from a place or on a type of equipment different from the place or type of equipment from where it, in fact, originated; or (2) modify, alter, or delete in any manner calling party

number information, originating point codes, or any other signaling information or call detail in connection with the transport and termination of traffic to the called party. See Section 2.16 of Netrix's Subscription Services Additional Terms Exhibit located at www.netrixglobal.com/contracts. Section 2.17 of these same Terms and Conditions provides Netrix with remedies against any of the foregoing prohibited uses, including, among other things, issuing warnings; terminating Client's Service, subscription, accounts, or users; and/or disabling access to or suspending the Service, subscription, or accounts. Netrix may take such action without notice to Client.

Know Your Upstream Provider. Netrix, through its underlying providers, has "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls. Set forth in Exhibit A hereto are the applicable procedures pursuant to Netrix's contracts with its underlying providers and the robocall mitigation plans filed by these providers.

Call analytics systems. Netrix analyzes high-volume voice network traffic to identify and monitor patterns consistent with robocalls. This information can assist in the traceback process to identify the source of illegal calls. Additionally, Netrix relies on the call analytics systems of its underlying providers, details of which are described in the Exhibit A below.

Traceback

Netrix will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use its service to carry, process, or originate robocalls.

EXHIBIT A

Applicable Contractual Terms with, and Procedures of, Netrix's Underlying Providers

Bandwidth.com

Prevention: Bandwidth has a stringent on-boarding screening process designed to proactively identify and prevent those that may engage in illegal robocalling from becoming Bandwidth customers at the outset. On-boarding screening procedures will always take Bandwidth's specific service provider role into account but the fundamentals of its on-boarding review procedures apply to all of Bandwidth's Intermediate, International Gateway and VSP services alike and we consider them to be the core of our "Know Your Customer" practices, which also inherently include "Know Your Upstream Provider" now in the context of the Commission's updated rules and terminology in wholesale service model scenarios (collectively "KYC"). Bandwidth tracks and records government enforcement actions and ever evolving industry trends to have up-to-date information on problematic use cases and known bad actors. Accordingly, Bandwidth requires that all of its upstream service providers (who may themselves be "Intermediate Providers", "Gateway Providers", "Originating Voice Service Providers" or "Foreign Service Providers") customers maintain valid registrations in the FCC's Robocall Mitigation Database ("RMD") and requires clear service-specific contractual requirements in which customers agree to cooperate with the ITG and agree to follow all applicable laws against illegal robocalling, fraud and abuse. After our initial "KYC" on-boarding screening, Bandwidth's operations personnel stay closely aligned with its customers and the industry's anti-robocalling efforts and developments to remind, educate and clarify what behaviors may signal or constitute unlawful robocalling, and continually notify customers when we identify instances that need their attention in order to prevent illegal robocalling behaviors on their networks.

Monitoring and Detection: Bandwidth has a team of operational experts who have implemented technical and operational processes and procedures to monitor, detect and analyze the use of its services and traffic on our network that helps to determine when illegal and inappropriate robocalling activity may be occurring. Bandwidth has developed and deployed a "Call Blocking Tool" that incorporates industry best practices into its core network to identify and block invalid, unallocated and otherwise obviously illegal telephone numbers. Further, even though it acts predominantly as an "Intermediate Provider", Bandwidth implemented STIR/SHAKEN in its all-IP core network infrastructure long before it was mandated by the FCC and has been working to increase call detail transparency and collaborative traceback enablement for years. When unlawful robocall campaigns are detected, Bandwidth follows established processes and procedures to notify upstream customers of the problematic traffic and request that they take immediate corrective actions to prevent reoccurrence of the illegal calls. Bandwidth's engagement and support for the ITG Tracebacks also includes work to monitor that its upstream providers are effectively cooperating with the ITG and working to address the sources of each traceback event. Bandwidth consistently analyzes its call detail records to identify problematic call patterns and their sources from where it sits in a myriad of traffic flows. Bandwidth then incorporates these learnings into its traffic data analytics and detection technologies to continually improve its capabilities to accurately detect suspected illegal activity and deploy mitigation measures.

Mitigation: Bandwidth's operations personnel are positioned to rapidly assist the ITG with the industry's collective efforts to identify the originating sources of illegal activities on the PSTN and prevent further delivery of unwanted and illegal traffic to the greatest degree possible. Bandwidth tracks its ITG request data and conducts considerable outreach to upstream customers that have sent traceback traffic to Bandwidth. Bandwidth's upstream provider mitigation efforts aim to achieve demonstrable

improvements in call quality, while also accounting for call quantities that are being serviced as well. When necessary and appropriate, Bandwidth can formally demand customers be put on a performance improvement plan, or if past mitigation efforts have failed, Bandwidth does take corrective action to terminate service arrangements that place Bandwidth and downstream providers and consumers at risk. Bandwidth's commitment to the benefits of STIR/SHAKEN in an all-IP network environment advances improvements in accurate and targeted call blocking that are designed to block calls from invalid and illegal telephone numbers in keeping with industry best practices and the FCC's recommendations, while simultaneously work to prevent anti-competitive and discriminatory blocking and mislabeling that is unfortunately plaguing the competitive industry with overly broad and blunt analytics. Bandwidth also works closely with Law Enforcement Agencies (LEA) at all levels of government and with its interconnected carrier partners. Bandwidth's fraud and security experts are constantly working to respond to complaints and trouble tickets with customers that may be associated with the unlawful uses of Bandwidth's services. In addition to these notifications, we then aim to work diligently together with our customers and other industry members to stop the unlawful robocall campaigns being detected. Finally, together with its active involvement in the ITG, Bandwidth supports the industry's established Do Not Originate (DNO) efforts pursuant to the industry best practices and procedures.

Lumen Technologies

Network Monitoring Practices: Lumen continuously monitors its networks for mass calling events and coordinates with other major providers, the ITG, trusted third parties (e.g., other peer service providers; end-user customer complaints), and key government agencies to address and mitigate obviously fraudulent calls. In coordination with the ITG, Lumen performs *Do Not Originate* (“DNO”) based upon a reasonable DNO list, which may include blocking of government impersonation calls. Since implementing its DNO framework in 2016 (prior to being required under the Commission’s rules), Lumen has conducted thousands of DNOs in response to alleged illegal robocalling campaigns identified by federal agencies, the ITG, or trusted third parties. Lumen also blocks “call back” *Direct Inward Dial* (“DID”) numbers used in government impersonation scam calls, including one-ring scams, and may block calls from numbers associated with mass robocalling scam campaigns as identified by trusted third parties or government agencies. In this regard, Lumen has taken action to suspend voice traffic from upstream providers in response to robocalling-related metrics observed by Lumen. Lumen stands ready to conduct additional network-level blocking of traffic from providers identified in Commission-issued Notifications of Suspected Illegal Traffic pursuant to 47 CFR § 64.1200 (n)(2) to the extent the recipients of those notifications fail to undertake the directed remedial measures.

Know-Your-Customer Initiatives: Lumen employs a variety of “know-your-customer” initiatives to help mitigate the risk that its customers would attempt to use Lumen’s network to initiate illegal robocalling campaigns. Lumen makes reasonable, good faith efforts to validate the identity of its customers, particularly smaller customers that may be more susceptible to identity theft. These measures include, but are not limited to, performing a credit check; requiring business customers to demonstrate that they are a legitimate business entity if they are not among the following: a Fortune 500 company, a public company, a state or federal government agency, or a major state university; and monitoring of financial position and payment performance. And since 2023, Lumen has required new customers and customers renewing their contracts to fill out a “know your customer” form. To comply with the Know-Your-Customer regulations set forth in the Patriot Act, all customers must be checked against the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) list of Specially Designated Nationals. To the extent applicable, customers are also checked against the FCC’s Robocall Mitigation Database. For Lumen’s foreign entities, Lumen additionally uses a third-party risk-screening service, designed for international business operations, to perform a variety of due diligence checks on its customers as part of the customer onboarding process. Collectively, these measures help prevent bad actors from becoming Lumen customers and reduce the likelihood that Lumen inadvertently carries illegal robocall traffic.

Telnyx LLC

Telnyx Customers, Monitoring, and Fraud Prevention: Telnyx collects contact and company information for each new customer upon sign-up. In line with our AUP and Terms and Conditions, Telnyx can leverage such contact information when we detect fraudulent call patterns to notify the customer of potential blocking or to pass such contact information to traceback administrators or law enforcement agents when necessary.

Telnyx takes the following steps to minimize the risk of fraud originating on our network. First, Telnyx blocks any subscribers who attempt to sign up with a “free-mail” account to reduce the risk of inviting bad actors onto our platform. Upon signing up with a valid e-mail, Telnyx customers are significantly limited to the amount of traffic they can originate from our platform. Suppose the customer wishes to increase their origination thresholds. In that case, they can apply for “level 2 verification,” which includes a more in-depth review of the company’s calling patterns, business model, and any previous complaints. Telnyx monitors traffic patterns, primarily tracking answer success rates (“ASR”) and average call duration (“ACD”), by all new and existing customers and immediately takes steps to block the account if the patterns mentioned above reflect fraudulent activity. In addition to internal monitoring tools, we have implemented a third-party analytics provider (Nomorobo) that monitors traffic patterns through machine learning to alert our fraud team of suspicious activity or calling patterns. Telnyx currently blocks any originating call with an invalid ANI and is in the process of implementing the US Telecom DNO list to ensure we catch any potential fraudulent call from leaving our platform. In addition to calling patterns, Telnyx has implemented payment method tracking to block any customer with suspicious payment activities.

Investigation of Suspicious Activity and Traceback: Telnyx always communicates with new and existing customers to share the latest FCC orders and industry best practices for complying with robocall mitigation technologies and minimizing fraud origination on our collective networks. As such, we have encouraged all our customers to participate in US Telecom’s Traceback group and have included these requirements in our services’ Terms and Conditions. Telnyx actively participates in Traceback requests and ensures to respond within 24 hours to all such requests from the Commission, law enforcement, and the industry traceback consortium. Any alert sent to Telnyx via our internal monitoring, tracebacks, and vendor alerts are properly reviewed by our fraud team, and a determination is made to remove the customer from our platform.

Blocking: Telnyx offers Inbound Call Screening to our customers, enabling users to flag and block unwanted incoming calls to maintain the integrity of their communications. Our Inbound Call Screening employs the SHAKEN/STIR attestation protocol to validate the authenticity of Caller ID information and includes two features – Enhanced Call Control and Spam Call Detection. With Enhanced Call Control, users can reject or flag suspicious calls based on customizable conditions. With our Spam Call Detection feature, users can effectively screen and identify potential spam calls to protect Telnyx numbers from unwanted solicitations and fraudulent activities, and avoid spam calls. As SHAKEN/STIR and other industry robocall mitigation efforts are implemented, we will be sure to monitor conditions for blocking fraudulent calls from reaching our customers.

IDT Telecom, Inc.

Only Accepting Traffic from Providers in the RMD: Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(e)(1), IDT accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers and Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(e)(2), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), IDT accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(e)(3), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), IDT accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD showing that the Gateway Provider has affirmatively submitted its filing and RMP, and (b) has not been de-listed pursuant to an enforcement action.

Blocking Calls on a Do-Not-Originate List: In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), IDT blocks calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan numbers. IDT has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number.

Analyzing and Monitoring Network Traffic Routing Through IDT's Network: Upon receiving call traffic, IDT also analyzes and monitors the call traffic that originates on, terminates to, or routes through IDT's voice network. Consistent with Principal No. 5 of the FCC's Caller ID Authentication Best Practices, IDT monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling.

In this regard, IDT has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, atypical call activity, and subscriber information), receive automatic alerts, investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis. When analyzing and monitoring call traffic, if IDT discovers call patterns that are consistent with illegal robocalling, IDT, after further investigation, takes appropriate action to address such behaviors, which may include working with the originating customer to resolve problematic traffic, blocking the problematic calls and/or terminating the customer's service.

Ensuring Foreign Providers Are Not Using IDT to Carry or Process High-Volume Illegal Traffic onto the U.S. Network: Pursuant to 47 C.F.R. § 64.1200(n)(4) and its January 16, 2023 effective date, when IDT serves as a Gateway Provider for voice traffic that is routing through its network, IDT takes reasonable and effective steps discussed under Section 5, above, to ensure that any Foreign Voice Service Provider or Foreign Intermediate Provider from which IDT directly receives traffic is not using IDT, as a Gateway Provider, to carry or process a *high volume* of illegal traffic onto the U.S. network. In addition, as a Gateway Provider, IDT blocks – to the best of its ability – foreign originating calls with U.S. North American

Numbering Plan numbers in the Caller ID, unless the upstream provider has been previously approved for sending such traffic, based on satisfactory due diligence.

Authenticating Voice Traffic: When operating as a Voice Service Provider, IDT does the following (1) authenticates and verifies caller identification information for all SIP calls that exclusively transit its own network; (2) authenticates caller identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path; and (3) verifies caller identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.¹⁰

When operating as a Gateway or Intermediate Provider, IDT authenticates caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call. ¹¹