

INTELEPEER ROBOCALL MITIGATION PLAN

February 27, 2026

Since the passage of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act,¹ the Federal Communications Commission (“FCC”) has adopted a series of new rules to combat illegal robo-calling traffic.² IntelPeer Cloud Communications, LLC and its affiliates³ (collectively “IntelPeer”) adopt this IntelPeer Robocall Mitigation Plan to outline the affirmative steps IntelPeer undertakes in its roles as a voice service provider, a gateway provider, and an intermediate provider, to avoid originating, carrying or processing illegal robocall traffic, through verifying the identity of its retail and wholesale customers and upstream providers, monitoring the traffic on its network, implementing STIR/SHAKEN in its network, collaborating with the state and federal governments and various industry groups, and updating our third-party contracts to reflect these requirements and measures.

IntelPeer serves retail enterprise customers and wholesale service provider customers (as registered with the FCC) using about a dozen domestic and international vendors. As such, IntelPeer acts as a Voice Services Provider and an Intermediate Provider in the market. Appendix A outlines the principals for IntelPeer Cloud Communications LLC. Unless otherwise expressly stated, the measures outlined in this Plan apply to IntelPeer, its operations and its treatment of traffic, in both roles of IntelPeer.

A. Third-Party Verification Processes

During the initial phase of account set-up and periodically throughout the business relationship, IntelPeer confirms the identity of any customers and voice vendors with which IntelPeer exchanges voice traffic domestically and internationally. This confirmation occurs through obtaining certain information about the entity and validating such information through government identification or other authentication controls prior to the execution of any service contract with such entity, pursuant to our third-party management policy. For all wholesale customers and our voice vendors, IntelPeer also validates the FCC 499A Filer ID number and Robocall Mitigation Database (“RMD”), which fulfills our obligations to “Know Your Customer” and “Know Your Upstream Services Providers” respectively. Lastly, any of our personnel that interact with our customers and vendors are also trained regularly on the importance of collecting, validating and capturing the pertinent information during the onboarding process and updating such information as needed.

¹ Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (TRACED Act).

² 47 C.F.R. §§64.6300-64.6308.

³ IntelPeer Holdings, Inc.

B. Network Monitoring

IntelPeer utilizes various calling platforms to support its suite of voice products, so different mechanisms are needed to identify suspicious use of calling numbers and suspicious traffic. Some of these calling platforms prevent our customers from asserting calling numbers, which were not issued by IntelPeer to that customer (or ported by that customer to IntelPeer), by natively screening those calling numbers. Alternatively, IntelPeer has other calling platforms that are more flexible and accommodate customers who may have procured numbers from other voice service providers.

Because of the different functionality of calling platforms, IntelPeer also employs strategies to monitor its network for suspicious number usage. Several of the modalities are described below, which IntelPeer uses with its retail enterprise customers as well as its wholesale customers where IntelPeer is the downstream intermediate provider. IntelPeer does not currently utilize any third-party analytics vendors in these modalities.

- **Do Not Originate ("DNO") Blocking:** IntelPeer maintains a DNO list consisting of the Industry Traceback Group (ITG) DNO list and a list of "impossible" numbers that IntelPeer derives from the LERG's definitions of valid exchanges in the North American Numbering Plan. IntelPeer revises the DNO list monthly as LERG updates are published, or whenever ITG announces an update to their DNO list. If a customer or voice service provider sends a call to the IntelPeer network where the From number is on the DNO list, IntelPeer blocks the call attempt.
- **DNO Alarming:** Outbound calls from retail enterprise customers are automatically examined to determine whether calls use numbers subject to DNO blocking. The system alerts IntelPeer personnel of matches. Although these calls get blocked by DNO blocking policies, and thus the blocked call attempts are not in themselves a threat to called parties, the call attempts can be an indicator of other unlawful traffic that was not blocked. This is because bad actors may use number rotation practices that spoof a combination of DNO numbers and From numbers that appear to be valid. The DNO calls are obvious to detect, whereas the bad actor's other calls are not. By investigating the overall traffic from the enterprise customer when a DNO call occurs, IntelPeer has detected and disrupted incidents where bad actors hacked customer calling platforms to generate scam and spam calls.
- **AI-powered Honeypot:** IntelPeer operates a honeypot, which is assigned a pool of inbound phone numbers that should never receive calls. The honeypot uses AI, text-to-speech, and speech-to-text technologies to engage in a conversation with the caller and ascertain call intent. In this way, the honeypot distinguishes between scam/spam calls and legitimate "wrong numbers." Furthermore, the honeypot uses network data to determine whether the call originated from the PSTN or from directly served IntelPeer customers. Honeypot calls initiated by IntelPeer retail enterprise customers result in an alert to IntelPeer personnel; personnel

investigate whether the call suggests a scam/spam campaign that needs to be disrupted. IntelPeer also uses the business intelligence gathered by the honeypot to design anti-spam methodologies to protect IntelPeer customers from inbound spam calls.

C. STIR/SHAKEN Implementation

IntelPeer is a voice service provider and an intermediate provider. When voice calls originate on the IntelPeer network, IntelPeer performs STIR/SHAKEN authentication to generate Identity headers and convey those headers downstream. For calls terminating on the IntelPeer network, IntelPeer performs STIR/SHAKEN verification on the upstream network's Identity header. For intra-network calls, IntelPeer's STIR/SHAKEN logic treats the call as having an originating leg and a terminating leg, which both happen to be on the IntelPeer network. Consequently, the originating leg follows the same STIR/SHAKEN authentication logic as an outbound internetwork call and the terminating leg follows the same STIR/SHAKEN verification logic as an inbound internetwork call.

In the capacity of a transit network, IntelPeer conveys to the downstream network any Identity header received from the upstream network. In this configuration, if IntelPeer receives an unauthenticated SIP invite from a wholesale customer, IntelPeer performs STIR/SHAKEN authentication to insert an Identity header into the SIP invite before conveying it to the downstream interconnecting network.

D. Traceback Requests

IntelPeer commits to continue responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within twenty-four (24) hours, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. IntelPeer also became a member of the Industry Traceback Group in July 2020, and has actively participated in the consortium's efforts to combat illegal robocalling.

In the past twenty-four (24) months, the traceback requests IntelPeer received are categorized as follows:

- Calls where IntelPeer was the intermediate service provider. For these cases, IntelPeer identifies the upstream service provider to ITG, and IntelPeer also directly notifies the interconnected network of the issue.
- Calls where the IntelPeer enterprise customer's calling platform was hacked, and the hacker exploits that vulnerability to generate calls. For these cases, IntelPeer immediately responds to ITG and works with the enterprise to stop the hacker's traffic. IntelPeer subsequently provides ITG with a summary of the root cause analysis and the corrective action to close the vulnerability.

- Calls that did not originate from or traverse the IntelPeer network. A different network referenced stale IP information when making their ITG submission, which erroneously attributed the upstream call source to IntelPeer.

E. Customer Contracts

IntelPeer includes clauses in its Master Services Agreements with customers that further combat illegal robocalling. Specifically, IntelPeer expanded the terms of our customers services agreement to obtain express authorization from all of our customers to fully respond to any traceback request from the Industry Traceback Group on suspected illegal robocalling activity. In addition to these contractual clauses directly associated with FCC actions, IntelPeer: (i) reserves the right to temporarily suspend or permanently terminate any Services or the Agreement entirely if we identify or reasonably suspect fraudulent activity or other violations of federal, state or local laws; and (ii) expressly prohibits any alteration, deletion or concealment of originating calling party information, originating ANI, originating point codes, nature of address, other signaling information, or call detail in any manner.

F. Regulatory Guidance and Industry Enforcement

IntelPeer closely monitors developments in guidance and enforcement actions regarding illegal robocalls at the federal and state level across the country. If IntelPeer becomes aware that a voice service provider is the recipient of a cease-and-desist letter from any regulator or state attorney general with respect to illegal robocall traffic anywhere, IntelPeer will promptly take steps to stop carrying any traffic from the offending voice service provider as allowed under the applicable rules, and maintains a list of such offending providers to avoid in our ongoing sales efforts.

G. Investigations or Enforcement of Suspected Illegal Robocalling

If IntelPeer determines that a customer may be involved in illegal robocalling using any of the above tools, IntelPeer personnel will conduct additional investigation, as needed, to ascertain whether the customer is generating illegal calls and brief the Executive Escalation Team on any confirmed activity. The Executive Escalation Team will determine the appropriate interventions to be taken to stop such traffic from originating on our network.

In the prior two years, IntelPeer has not been the subject of a formal actions by law enforcement or any regulatory agency due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

APPENDIX A: List of Principals

Principal Name	Title	Date of Appointment
Frank Fawzi	President and Chief Executive Officer	October 21, 2013
Andre Simone	Secretary and Chief Operating Officer	November 15, 2023