November 19, 2018

VIA ECFS and E-Mail

Chairman Ajit Pai
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Status of Caller ID Authentication Implementation
Call Authentication Trust Anchor, WC Docket No. 17-97

Dear Chairman Pai:

I appreciate the opportunity to respond on behalf of Vonage Holdings Corp. to your questions directed to our CEO, Alan Masarek, regarding our progress in implementing a verified caller ID framework.[1] Vonage is a strong proponent of efforts to combat unwanted robocalls and caller ID spoofing. To that end, Vonage has concrete plans to implement authenticated caller ID in 2019, consistent with the timeline proposed by the North American Numbering Council. As your letter recognizes, establishing a robust call authentication framework has required the development of protocols and standards, along with the creation of a Governance Authority and the selection of a Policy Administrator. Vonage has elected to participate in the policy development process in cooperation with other VoIP providers through the VON Coalition. Although the development process is ongoing, we are laying the groundwork at Vonage now to sign calls and work with the system established by the Policy Administrator as soon as it is established. Below, please find responses to your specific questions:

- *What is preventing or inhibiting you from signing calls today? What is your timeframe for signing (i.e., authenticating) calls originating on your network?*

As detailed below, Vonage has begun the process of implementing the SHAKEN/STIR framework throughout our network, and we expect to begin authenticating calls originating on our network prior to the end of 2019. Vonage participates in the Secure Telephone Identity Governance Authority through the VON Coalition, and we continue to monitor the development of appropriate certificate-related policies, as well as the selection of the Policy Administrator. Although that industry collaboration is still in

[1] Letter from Chairman Ajit Pai, Federal Communications Commission, to Alan Masarek, Chief Executive Officer, Vonage (Nov. 5, 2018).

23 Main Street • Holmdel, New Jersey 07733
Tel: 732-528-2600 • Fax: 732-203-7897

progress, we are developing our internal solutions on a schedule that we expect will allow Vonage, when acting as a terminating carrier, to verify certificates once the certificate repository is in place.

- *What tests have you run on deployment, and what are the results?*

We are in the process of finalizing the design and procedures for our tests, and we expect to have results in Q2 of 2019. To manage the testing process as efficiently as possible, Vonage is working with standards organizations, industry partners, and fellow members of the VON Coalition to collaborate and share best practices and resources. For example, Vonage is in the process of acquiring access to the Alliance for Telecommunications Industry Solutions ("ATIS") Robocalling Testbeds, which is hosted by the Neustar Trust Lab. Vonage has signed the Non-Disclosure Agreement for the ATIS Testbeds and has signed the Robocalling Test Use Policy. Working cooperatively now with the Neustar Trust Lab and our industry partners will help ensure that the final form of our SHAKEN/STIR implementation aligns with leading industry standards.

- *What steps have you taken to work with vendors to deploy a robust call authentication framework?*

We are exploring options for appropriate vendors, and we expect to finalize our selections in 2018 or early 2019. For example, we are working with our primary session border control vendor, Sonus Networks, Inc. (d/b/a Ribbon Communications Inc.), to identify the most appropriate solutions for Vonage's network. Members of Vonage's engineering team are scheduled to attend the Robocall Summit at the SIP Forum's 2018 SIP Network Operators Conference in December 2018. In addition to identifying and sharing best practices for implementing the SHAKEN/STIR Framework, our team has planned to and will use the conference as an opportunity to engage with appropriate vendors.

- *How often is Vonage an intermediate provider, and do you intend to transmit signed calls from other providers?*

Vonage's role as an intermediate provider is very limited. At this time, we only serve as an intermediate provider for Nexmo, which is Vonage's Application Programming Interface Platform. We do intend to transmit signed calls originating with Nexmo. Vonage's Nexmo business unit enforces robust "know your customer" policies that help Vonage authenticate calls originating with Nexmo. Before a customer can send large volumes of traffic or make deposits, the customer must go through an individualized one-on-one interaction with the Vonage team, which then verifies the customer's use cases for the service and that it is a legitimate business. This ensures that customers of Nexmo are complying with acceptable use policies related to Nexmo. Vonage does not provide wholesale services to any other entity or client.

- *How do you intend to combat and stop originating and terminating illegally spoofed calls on your network?*

As discussed above, we are taking steps to implement the SHAKEN/STIR framework within our network during 2019. Consistent with those efforts, we will be able to provide full attestation from calls originating from Vonage customers. Through the VON Coalition, we continue to participate in and monitor the industry's selection of rules governing the issuance and use of Secure Telephone Identity (STI) certificates and its selection of an administrator to implement STI policies. Once the administrator is in

place (which we anticipate will be in 2019), Vonage will be able to verify terminating calls against the certificate repository.

We also recognize that protecting our customers from spam calls requires a multifaceted approach. Vonage is committed to providing its customers with cutting-edge solutions to their communications needs, and in that regard we already offer Spam Shield, a Vonage program that checks incoming calls against a dynamic database of numbers associated with telemarketing, robocalls, and scam. If Spam Shield finds a match, it displays "suspected spam" on the customer's caller ID and allows them to decline the call and add the number to a custom block list. Spam Shield is based on the program "Nomorobo," which won the Federal Trade Commission's Robocall Challenge in 2013 for Best Overall Solution for blocking illegal robocalls. While "blacklist" solutions like Spam Shield cannot prevent one hundred percent (100%) of unwanted calls, they are helping to combat the problem today and will complement verified caller ID solutions in the future.

- *The Commission has already authorized voice providers to block certain illegally spoofed calls. If the Commission were to move forward with authorizing voice providers to block all unsigned calls or improperly signed calls, how would you ensure the legitimate calls of your customers are completed properly?*

As explained above, Vonage fully expects to implement caller ID authentication by the end of 2019, pursuant to industry standards and guidelines and will be able to signal the appropriate level of attestation for its users' outbound calls at that time.

* * * * *

We share your concern and appreciate the Commission's efforts to combat unwanted robocalls and caller ID spoofing. As detailed above, work at Vonage is underway to implement caller ID authentication by the end of 2019. We would be pleased to answer any additional questions Commission staff may have. Please do not hesitate to contact me at 732-444-4613.

Respectfully submitted,

Randy K. Rutherford
Chief Legal Officer
Vonage Holdings Corp.
23 Main Street
Holmdel, NJ 07733

CC: Deborah Salons, FCC
Alan Masarek, Vonage CEO