

November 30, 2017

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: *Structure and Practices of the Video Relay Service Program*, CG Docket No. 10-51;
*Telecommunications Relay Services and Speech-to-Speech Services for Individuals with
Hearing and Speech Disabilities*, CG Docket No. 03-123

Dear Ms. Dortch:

Sorenson Communications, LLC (“Sorenson”) writes in response to the recent *ex parte* filed by Neustar, which memorializes—nearly two months late—a meeting between Neustar and Commission staff. At the meeting, Neustar proposed a new requirement on Deaf users of public videophones and significant work for VRS providers to retrofit their videophones. Neustar proposed that any Deaf user that may have a future requirement to use a public VRS phone would need to carry or have memorized some form of credential, on the chance they would be in a situation that required the use of a videophone located in public spaces or in businesses. Implied in this requirement is that if you are Deaf and do not have your credentials, you have no right to use such a device. The sole purpose of this proposed overly burdensome and expensive technical mandate is to eliminate the possibility that an ineligible user, who knows ASL, could place such a call.

As Sorenson explained in its opening comments,¹ forcing users to log in before placing calls is a burdensome and expensive solution to a problem that does not exist. Sorenson already requires all users who place a VRS call from a public phone to digitally sign a self-certification indicating that they are deaf or hard of hearing and need VRS in order to communicate,² preventing any inadvertent misuse of the phone. Because Deaf and hard-of-hearing persons are

¹ See Comments of Sorenson, Communications, LLC Regarding Part III and Sections IV.C-E and G-H of the Further Notice of Proposed Rulemaking at 19-20, CG Docket Nos. 03-123 and 10-51 (filed May 30, 2017) (“FNPRM”).

² The self-certification reads: “By clicking the ‘Accept’ button, you hereby certify that you have a hearing or speech disability and need VRS to be able to communicate with other people. You understand that the cost of VRS calls is paid for by contributions from other telecommunications users to the TRS Fund. You further attest by clicking the ‘Accept’ button that you are eligible to use VRS.”

eligible and thus entitled to use VRS, so long as the person is Deaf or hard-of-hearing, there is no issue of ineligible use.

And there is neither an incentive nor an opportunity for hearing users to place a VRS call. Hearing users have no reason to place a call through a VRS interpreter. The vast majority of Americans in a public place that would have a VRS public phone have cell phones, and can simply dial a call directly to talk to whomever they wish. In any event, if they do not use ASL, they functionally cannot use a VRS phone. Fraudulent use of a public VRS phone would have to be a call placed from a hearing person, through a VRS Video Interpreter, to another hearing person: point-to-point calls from a hearing person to a Deaf or hard-of-hearing person would be point-to-point calls permissible under the FCC's rules. But such a call is extremely unlikely to ever occur because, unlike with IP Relay, which allows complete anonymity for users that may or may not use ASL, VRS requires the user to appear on video and communicate in ASL. Moreover, as the NPRM correctly recognizes, "given that most hearing people are not fluent in ASL,"³ even if a hearing user wanted to use VRS, the VRS interpreter would realize that the user is unable to communicate in ASL and would terminate the call as non-compensable. The presence of the VRS interpreter provides a crucial additional safeguard against an ineligible user placing such a call, which should not be discounted.

At the same time, forcing users to log in before placing calls would place significant burdens on deaf users, who will be required to memorize logins and passwords whenever they want to use a public or enterprise phone. This burden would weigh the heaviest on the most vulnerable populations: the elderly, children, and individuals with cognitive and learning disabilities. By enforcing this requirement, the Commission would deprive these populations of functionally equivalent service. Further, the Commission would make it difficult or impossible for public phones to process emergency calls and incoming and returned calls, including returned calls from emergency responders.

In addition to the problems inherent in requiring users to log in, users would also be burdened because the OAuth specification requires the use of a system web browser, which Sorenson's purpose built VRS videophones do not have. Sorenson's VRS videophones are considered "Browserless and Input Constrained Devices" under the OAuth 2.0 protocol.⁴ Accordingly, to meet the security requirements of OAuth 2.0, users would be required to perform the authorization on a secondary device,⁵ such as a smartphone. But users who have ready

³ FNPRM at ¶ 119.

⁴ <https://tools.ietf.org/html/draft-ietf-oauth-device-flow-07.pdf>

⁵ OAuth 2.0 Threat Model and Security Considerations states, in part:

Client developers should not write client applications that collect authentication information directly from users and should instead delegate this task to a trusted system component, e.g., the system browser.

access to a smartphone do not need to use a public phone (they can place VRS calls on their smartphone using providers' VRS apps); thus, the, OAuth protocol would make public phones inaccessible to the only users who need them.

In addition to the burdens imposed on users, and apart from the fees that Neustar would charge to design and run its proposed proxy server, implementing OAuth will impose significant costs on providers, who would have to create and deploy OAuth servers and retrofit their phones to support the OAuth protocol. Modifying phones and backend systems to add OAuth capability, even if possible, would require providers to take staff off other projects and spend time to make the changes. Sorenson estimates that the cost of creating, testing, and deploying an OAuth authorization server and modifying and testing videophone software would be over \$1 million and would require about four to six months of engineer time. Sorenson would also have to implement these changes on mobile and desktop endpoints, adding to the already significant costs. These costs would be in addition to the other costs imposed by the login requirement. The login requirement would force Sorenson to spend between \$1-2 million to develop and maintain new user interfaces for enterprise and public phones, develop and deploy OAuth servers, and to distribute usernames and passwords.

Not only will using the OAuth protocol be costly for companies; it could potentially be costly for users and ultimately the TRS Fund. Numerous commentators have identified significant security vulnerabilities in OAuth and other third-party authentication applications.⁶ Among other things, these vulnerabilities could leave VRS users open to hacks that could expose their usernames and passwords and make them vulnerable to identity theft—particularly if they reuse their passwords across multiple sites.

The Commission should not require providers to spend millions of dollars to implement the OAuth framework or implement any login requirement without first doing a cost-benefit analysis. On the present record, the costs of such a proposal greatly exceed any benefit. Accordingly, Sorenson urges the Commission to reject these proposals.

Sincerely,



John T. Nakahata
Counsel to Sorenson Communications, LLC

See RFC 6819 OAuth 2.0 Threat Model and Security Considerations (January 2013) at 20 available at <https://www.rfc-editor.org/rfc/pdf/rfc6819.txt.pdf>

⁶ <https://www.scmagazineuk.com/researchers-find-two-flaws-in-oauth-20/article/532045/>; <https://threatpost.com/oauth-2-0-hack-exposes-1-billion-mobile-apps-to-account-hijacking/121889/>; <http://www.securityweek.com/oauth-20-vulnerability-leads-account-takeover>; <https://www.sans.edu/downloads/group-project-jan17-2.pdf>