neustar

December 13, 2017

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Room TW-A325
Washington, D.C. 20554

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

Dear Ms. Dortch:

On November 15, 2017, Neustar, Inc. ("Neustar"), as the Internet-based Telecommunications Relay Service ("iTRS") Telephone Number Directory ("iTRS Directory") Administrator filed, at the request of Commission staff, an *ex parte* letter describing how to allow the login of an authorized iTRS user to a public Video Relay Service ("VRS") device, where the default iTRS provider of the device was not the default provider of the user. In a November 30, 2017 *ex parte* letter, Sorenson Communications, LLC ("Sorenson") responded to Neustar's letter questioning the rationale for requiring logins to public devices and raising several technical objections to the recommended approach of using OAuth Relay as the mechanism to accomplish the login capability. This letter responds to Sorenson's technical concerns; Neustar takes no position on the merits of whether such logins for public videophones should be required.

Sorenson's first concern is that the OAuth 2.0 specifications require the use of a system web browser, which its VRS videophones do not have. Sorenson is correct that having a web browser would be a requirement of any public VRS device if OAuth 2.0 was required for login. VRS devices that do not have a web browser, or are not upgraded to have a minimal web browser, could not be used as public VRS devices. Since many VRS devices are already equipped with such browsers,[1] the browser requirement only moderately limits the VRS device choices available for an iTRS provider to deploy in a public setting. Neustar does not expect non-browser equipped devices to be used in these settings, nor does Neustar expect secondary devices to be used to authenticate users on public VRS devices.

Neustar believes that Sorenson confuses the capabilities and costs needed to support OAuth. A public VRS device needs only a simple web browser, as well as a rudimentary mechanism to invoke the proper URL when a login is required. iTRS providers that wish to offer public VRS

[1] For example, the ZVRS Z70 includes a browser and any of the software based Windows/Mac videophones such as Purple P3, Convo for Mac/PC and Global VRS for Windows have browser support.

device capability (i.e., be the default provider for one or more public VRS devices) will need to modify their central systems to know that login to a public device is needed, trigger the web browser to visit the correct URL, and only allow calls to/from public VRS devices that have logged in users.

All iTRS providers, even those not offering public devices, would be required to create a single central OAuth server that authenticates their users when invoked by the Neustar OAuth proxy.[2] Neustar believes that many providers already utilize username/password for user access to existing functionality that can be extended to OAuth. Providers that do not have such capability would need to develop it. Open source code is available to make the cost of implementing OAuth servers and username/password capability, if not already in use, modest for the iTRS providers to implement.[3]

Finally, although there are no entirely secure systems, OAuth 2.0 has undergone significant security analysis and is regarded to be a very secure mechanism.[4] The studies cited by Sorenson involve extensions Identity Providers made to the OAuth protocol or poor third-party implementations of that protocol. Neustar is not proposing that any extensions be used and, as an expert in network security, Neustar does not expect its implementation to be poor.[5] There is no question that Sorenson is correct that users who reuse passwords are vulnerable to having credentials stolen from one site being used on another site. Unfortunately, this is true of any login system and is not unique to OAuth 2.0.

Respectfully submitted,

Richard L. Fruchterman, III
Sr. External Affairs Counsel

cc: David Schmidt
Eliot Greenwald
Andrew Mulitz
Diane Mason
Karen Peltz Strauss
Robert Aldrich
Michael Scott

---

[2] Neustar only plays a role in OAuth to enable the authentication system to function in a manner that prevents iTRS providers from capturing information about the users of other iTRS providers.
[3] *See,* https://oauth.net
[4] *See, e.g.*, https://pdfs.semanticscholar.org/d097/bd22b1ae7e0ae157f9cba54df1810fbdf9b9.pdf.
[5] If added to the modification of the iTRS Directory Administrator contract that will be necessary to implement OAuth Relay, Neustar can assist iTRS providers with the security of their implementations of OAuth 2.0.