



August 5, 2019

Via ECFS and Hand Filing

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

Re: Request for Confidential Treatment – *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”) hereby submits the attached comments, titled Comments of Sorenson Communications, LLC in Response to the Further Notice of Proposed Rulemaking (“Comments”).

Sorenson requests pursuant to Sections 0.457 and 0.459 of the Commission’s rules, 47 C.F.R. §§ 0.457, 0.459, that the Commission withhold from any future public inspection and accord confidential treatment to the confidential, business sensitive information contained in the attached Comments.

The Confidential Information constitutes highly sensitive commercial information that falls within Exemption 4 of the Freedom of Information Act (“FOIA”). Exemption 4 of FOIA provides that the public disclosure requirement of the statute “does not apply to matters that are... (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential.” 5 U.S.C. § 552(b)(4). Because Sorenson is providing commercial information “of a kind that would not customarily be released to the public,” this information is “confidential” under Exemption 4 of FOIA. *See Critical Mass Energy Project v. NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992). Because this is a voluntary filing, if the Commission denies this request for confidential treatment, Sorenson requests for its Confidential Information to be returned.

In support of this request and pursuant to Section 0.459(b) of the Commission’s rules, iconectiv hereby states as follows:

1. Identification of the Specific Information for Which Confidential Treatment Is Sought (Section 0.459(b)(1))

Sorenson seeks confidential treatment with respect to the Comments.

Ms. Marlene H. Dortch

August 5, 2019

Page 2 of 3

2. Description of the Circumstances Giving Rise to the Submission (Section 0.459(b)(2))

Sorenson is voluntarily submitting the Comments.

3. Explanation of the Degree to Which the Information Is Commercial or Financial, or Contains a Trade Secret or Is Privileged (Section 0.459(b)(3))

The information described above merits confidential treatment because it constitutes confidential commercial information. Sorenson does not disclose this information publicly, and competitors could use this information to unfairly target users or otherwise compete with Sorenson.

4. Explanation of the Degree to Which the Information Concerns a Service that Is Subject to Competition (Section 0.459(b)(4))

The VRS market is highly competitive throughout the United States.

5. Explanation of How Disclosure of the Information Could Result in Substantial Competitive Harm (Section 0.459(b)(5))

Disclosure would result in competitive harm because it would offer competitors insights about Sorenson's business activities.

6. Identification of Any Measures Taken to Prevent Unauthorized Disclosure (Section 0.459(b)(6))

Sorenson does not make this information publicly available, nor has it authorized its employees to release this information to the public.

7. Identification of Whether the Information Is Available to the Public and the Extent of Any Previous Disclosure of the Information to Third Parties (Section 0.459(b)(7))

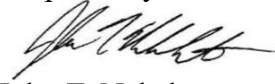
Sorenson has not previously disclosed the information publicly.

8. Any Other Information That the Party Seeking Confidential Treatment Believes May Be Useful in Assessing Whether Its Request for Confidentiality Should Be Granted (Section 0.459(b)(9))

Data subject to this request also would qualify for Exemption 4 of the Freedom of Information Act. Exemption 4 protects information that is (i) commercial or financial; (ii) obtained by a person outside of the government; and (iii) privileged or confidential. 5 U.S.C. § 552(b)(4).

Ms. Marlene H. Dortch
August 5, 2019
Page 3 of 3

Respectfully submitted,



John T. Nakahata
Christopher J. Wright
Mark D. Davis
Stephen W. Miller
Mengyu Huang
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1300
jnakahata@hwglaw.com

Counsel for Sorenson Communications, LLC

Attachment

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20544

In the Matter of:

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

COMMENTS OF SORENSON COMMUNICATIONS, LLC IN RESPONSE TO THE
FURTHER NOTICE OF PROPOSED RULEMAKING

John T. Nakahata
Christopher J. Wright
Mark D. Davis
Stephen W. Miller
Mengyu Huang
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1300
jnakahata@hwglaw.com

Counsel for Sorenson Communications, LLC

August 5, 2019

Table of Contents

SUMMARY AND INTRODUCTION	1
ARGUMENT	4
I. The Commission Should Allow VRS Providers to Provide Service to New and Porting Users for Up to Two Weeks Pending TRS-URD Verification	4
II. The Commission Should Not Impose Costly, Burdensome, and Unnecessary Log-in Requirements on the Use of Public and Enterprise Videophones	5
A. A Log-in Requirement Would Burden VRS Users and Undermine Functional Equivalency	5
B. A Log-in Requirement Would Fail to Meaningfully Reduce Waste, Fraud, or Abuse to Justify Its Significant Regulatory Burdens.....	6
C. Neustar’s Proposed OAuth Log-in Procedure is Prohibitively Expensive and Technically Infeasible	10
D. Sorenson’s Proposed Alternative Would Impose Less Regulatory and Technical Burdens than the Log-in Requirement, While Still Accomplishing the Commission’s Goal of Fraud Prevention	15
CONCLUSION	17

**COMMENTS OF SORENSON COMMUNICATIONS, LLC IN RESPONSE TO THE
FURTHER NOTICE OF PROPOSED RULEMAKING**

Sorenson Communications, LLC (“Sorenson”) hereby comments with respect to Sections IV.B-C of the Further Notice of Proposed Rulemaking regarding Video Relay Services (“VRS”).¹

SUMMARY AND INTRODUCTION

Sorenson applauds the Commission’s ongoing efforts to improve VRS service while safeguarding against waste, fraud, and abuse. In doing so, the Commission should take care not to impose costly regulation that would overburden VRS users and providers and undermine the functional-equivalence requirement of the Americans with Disabilities Act (“ADA”), all while resulting in negligible benefits. With this principle in mind, Sorenson supports the FNPRM’s proposal to allow VRS providers to receive compensation for providing service to new and porting users for up to two weeks pending the completion of TRS-URD verification. We agree that this rule change would eliminate the possibility of “unnecessary inconvenience to VRS registrants,” protecting them from undue delay or service disruption as they commence VRS service or switch providers, “without a significant increase in the risk of waste, fraud, and abuse.”² As proposed, the rule change also helps ensure that VRS providers are delivering functionally equivalent service by treating VRS users more like hearing users who initiate or port service.

¹ *Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, Report and Order and Further Notice of Proposed Rulemaking, FCC 19-39, CG Docket Nos. 10-51 and 03-123 (rel. May 15, 2019) (“*Report and Order*” or “*FNPRM*”).

² *Id.* ¶ 55.

Functional equivalence also leads Sorenson to oppose the FNPRM’s proposed log-in requirement for enterprise and public videophones.³ First, we reiterate our concerns that the log-in requirement would unreasonably burden VRS users and undermine functional equivalency. The FNPRM sidesteps consumer concerns that the log-in procedure would require consumers to provide sensitive personally identifiable information to providers, exposing them to heightened risks of privacy and security violations. The FNPRM also underestimates the burdens to consumers from having to memorize challenging passcodes or PINs, particularly when those most likely to depend on public and enterprise phones for their communication needs—including the elderly, homeless, children, and users with cognitive disabilities—are the likeliest to struggle with remembering or even figuring out how to enter a password. Similarly, these groups are the likeliest to lack regular access to smartphones, voicemail, email, or other devices and accounts requiring routine password memorization.

Second, the log-in requirement remains “a solution in search of a problem.”⁴ The record contains no evidence of misuse of public or enterprise phones. Existing data and common sense both suggest, at most, a negligible risk that these phones will be used to place ineligible calls, given that users must converse in ASL and hearing persons have more convenient, low-cost alternatives to VRS (such as mobile phones) for placing calls. The FNPRM fails to establish that the benefits would outweigh the costs of implementation, particularly where less-burdensome alternatives exist to accomplish the Commission’s goals of preventing waste, fraud, and abuse.

³ *Id.* ¶¶ 58-59.

⁴ 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, CG Docket Nos. 10-51 and 03-123 (filed May 30, 2017) (“Sorenson May 30, 2017 Comments”); *see* Letter from John T. Nakahata, Counsel for Sorenson, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 1 (filed Nov. 30, 2017) (“Sorenson Nov. 30, 2017 Ex Parte”).

Third, the proposed log-in procedure would follow the OAuth 2.0 standard, rendering it not only prohibitively expensive but also technically infeasible. Sorenson's current public and enterprise videophones cannot be modified to support a system web browser, as required to fully and securely implement OAuth 2.0. As a result, replacing all of Sorenson's unmodifiable public and enterprise videophones would cost a total of \$25 million to \$37 million. This includes approximately \$2 million to \$3 million for public videophones and \$23 million to \$34 million for enterprise videophones. Moreover, the proposed alternatives to a system web browser would undermine functional equivalency or expose users and providers to serious security vulnerabilities. The security risks are especially prevalent in the supposed "streamlined" version of OAuth, which, in fact, does not meet the OAuth security standard and is a purely hypothetical concept untethered to any industry-accepted authorization protocol standard.

As an alternative to the log-in requirement, the Commission should implement self-certification through a digital signature for all VRS users before they can use a public or enterprise videophone for a VRS call. Should the Commission require additional precautions, it could require VRS users to enter their VRS phone numbers, instead of a passcode or PIN. This would implement a data-driven approach where the TRS Fund Administrator would monitor usage trends for potential fraud and investigate further where necessary. However, we note that such a requirement would still not be functionally equivalent, and could deny access to public phones for Deaf individuals who cannot receive VRS where they live—for example, because of a lack of adequate broadband services. Nonetheless, these alternatives are more easily administrable than the proposed log-in requirement and would help prevent waste, fraud, and abuse while placing a much lower burden on consumers. At minimum, given the significant

financial and technical hurdles faced by Sorenson to implement OAuth, the Commission should exempt Sorenson’s unmodifiable public and enterprise videophones from the log-in requirement.

ARGUMENT

I. THE COMMISSION SHOULD ALLOW VRS PROVIDERS TO PROVIDE SERVICE TO NEW AND PORTING USERS FOR UP TO TWO WEEKS PENDING TRS-URD VERIFICATION.

Sorenson supports the FNPRM’s proposed rule to allow VRS providers to provide service to new and porting users for up to two weeks pending the completion of identity verification.⁵ We agree that this change would help ensure that new and porting VRS users can utilize VRS services without undue delay or service disruption, would facilitate competition by reducing switching costs, and would align with the goals of functional equivalence.⁶ As VRS providers have explained, this two-week period would ensure that providers treat VRS users more like hearing users who initiate or port service, where service typically commences immediately.⁷ The rule change also would protect consumers from service disruption or delay caused by verification issues that are often outside of the consumer’s control, such as outage or technical issues experienced by third parties in the verification process (*e.g.*, the TRS-URD Administrator or LexisNexis database).⁸ Additionally, the FNPRM correctly recognizes that “any resulting risk of waste, fraud, or abuse is minimal” since “no compensation may be

⁵ *FNPRM* ¶¶ 55-57.

⁶ *Id.* ¶ 55; *see also* Comments of Telecommunications for the Deaf and Hard of Hearing, Inc., et al., CG Docket Nos. 10-51 and 03-123 (filed July 26, 2018).

⁷ Joint Petition of VRS Providers for a Waiver at 2, 7, CG Docket Nos. 10-51 and 03-123 (filed June 20, 2018) (“VRS Providers Petition”).

⁸ *Id.* at 8.

requested or paid until the user’s identity has been verified.”⁹ The benefits clearly outweigh any costs, and we encourage the Commission to act promptly to implement this rule change.

II. THE COMMISSION SHOULD NOT IMPOSE COSTLY, BURDENSOME, AND UNNECESSARY LOG-IN REQUIREMENTS ON THE USE OF PUBLIC AND ENTERPRISE VIDEOPHONES.

A. A Log-in Requirement Would Burden VRS Users and Undermine Functional Equivalency.

Sorenson reiterates its opposition to the FNPRM’s proposed log-in requirements for individuals using public and enterprise videophones for VRS calls.¹⁰ The Commission cannot brush aside the log-in requirement’s significant burdens to consumers that conflict with functional equivalency.¹¹ Repeatedly, consumer groups have stressed the unreasonable burden the log-in requirement would place on Deaf and Hard-of-Hearing users.¹² VRS users would have to provide sensitive personally identifiable information to providers, thereby increasing their risks for identity theft, and memorize challenging passcodes or PINs.¹³

Consumer groups also have reiterated that the log-in requirements “would be a move away from functional equivalency,” the guiding principle for Telecommunications Relay

⁹ FNPRM ¶ 57; *see also* VRS Providers Petition at 10.

¹⁰ FNPRM ¶¶ 58-59.

¹¹ *See id.* ¶ 62 and ¶ 62 n.173.

¹² *See, e.g.*, Letter from Danielle Burt and Tamar Finn, Counsel for Telecommunications for the Deaf and Hard of Hearing, Inc., to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 1-2 (filed Feb. 20, 2018) (“Consumer Groups Feb. 20, 2018 Ex Parte”) (citing privacy and security concerns from Consumer Groups’ Joint Petition, CG Docket Nos. 10-51 and 03-123 (filed October 1, 2015)); Comments of Consumer Groups on Notice of Inquiry and Further Notice of Proposed Rulemaking at 5-6, CG Docket Nos. 10-51 and 03-123 (filed May 30, 2017) (“Consumer Groups May 30, 2017 Comments”).

¹³ *Id.*

Services (“TRS”), including VRS.¹⁴ Hearing users can simply pick up a public or enterprise phone to access the critical communications services they need, without having to clear the extra hurdles of logging-in and placing themselves at heightened security risk.¹⁵

In response, the FNPRM assumes that the log-in requirement would only impose “minor” burdens on users because “[i]ndividuals use log-ins regularly to access smartphones, voicemail, and email, as well as work, school, and personal computers, and commercial, retail, and financial accounts,” where they “routinely need to remember (or store in a retrievable location) usernames, passwords, and PINs.”¹⁶ But this improperly minimizes consumers’ legitimate privacy and security concerns. Similarly, it fails to address the problem that those consumers who are most likely to depend on public phones—the elderly, the homeless, children, those with cognitive disabilities, and those without access to mobile VRS devices or functioning VRS equipment at home, among others—are also the least likely to regularly access smartphones, voicemail, email, computers, and commercial, retail, and financial accounts. The log-in requirement’s burdens would especially harm these vulnerable groups.¹⁷

B. A Log-in Requirement Would Fail to Meaningfully Reduce Waste, Fraud, or Abuse to Justify Its Significant Regulatory Burdens.

The Commission cannot justify the proposed log-in procedure by claiming that consumer burdens would be offset by its “substantial benefit in preventing the misuse of enterprise and

¹⁴ Consumer Groups May 30, 2017 Comments at 2, 6.

¹⁵ See *infra* Section II.C for a discussion of the security risks that VRS users would face as a result of the Neustar’s proposed log-in procedure.

¹⁶ FNPRM ¶ 62.

¹⁷ See Letter from John T. Nakahata, Counsel for Sorenson Communications, LLC, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 4 (filed Jan. 22, 2018) (“Sorenson Jan. 22, 2018 Ex Parte”); Consumer Groups Feb. 20, 2018 Ex Parte at 1-2; Sorenson May 30, 2017 Comments at 4, 22.

public videophones,”¹⁸ when the record suggests precisely the opposite. The record remains devoid of evidence that *any* such misuse is occurring, much less at a level that would warrant the proposal’s costs to consumers and providers. First, the misuse examples cited in the FNPRM primarily consist of past “minute pumping” schemes that predated mandatory FCC certification of VRS providers and the ban on “white label” non-certified subcontractors.¹⁹ Those actions long ago ended minute pumping schemes, as certified VRS providers are directly accountable for their minutes and report them to the TRS Administrator. The Commission does not point to any specific case where an ineligible user attempted to use a public or enterprise phone to place a VRS call. These types of fraud are extremely unlikely given the need to communicate through ASL, the interposition of the video interpreter, and the lack of any plausible incentive for an ASL-capable hearing user to do so in an era of widespread cellphone use with distance-insensitive large minute buckets or unlimited calling plans.²⁰

Additionally, enterprises will be certifying responsibility for enterprise phones that may be in settings where they are used by more than a few individuals.²¹ The Commission has no basis for assuming that enterprises will be unable to effectively police use and prevent the hypothesized minute-pumping abuse. Similarly, the Commission has no basis for assuming that other registration and monitoring requirements already in place—including URD registration,

¹⁸ FNPRM ¶ 62.

¹⁹ See *id.* ¶ 58 n.166 (citing past minute pumping schemes); *Structure & Practices of the Video Relay Services Program*, Report and Order and Further Notice of Proposed Rulemaking, FCC 11-54, CG Docket No. 10-51, 26 FCC Rcd. 5545, 5570-75 ¶¶ 47-61 (2011) (discussing and amending rules to prohibit “white label” non-certified subcontractors).

²⁰ See Letter from John T. Nakahata, Counsel for Sorenson, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 3 (filed Jan. 26, 2018) (“Sorenson Jan. 26, 2018 Ex Parte”); Sorenson Nov. 30, 2017 Ex Parte at 2; Sorenson May 30, 2017 Comments at 19-20.

²¹ See *Report and Order* ¶¶ 28-29.

Sorenson’s mandatory annual training for all employees making clear that they cannot accept or make fraudulent calls, training for VRS interpreters to watch for and report fraud and to disconnect VRS calls when the caller is a hearing person, and the recently enacted requirement that VRS providers monitor enterprise and public videophone usage and to report any “unusual activity” to the TRS Fund administrator—will be unable to effectively police and prevent such abuse. The Commission should reduce the burdens placed on VRS users to achieve functional equivalency, not construct additional hurdles in response to hypothetical harms.

Without any concrete example of public or enterprise phone misuse, the FNPRM asserts as “sufficient” justification for a log-in requirement “that total usage of enterprise and public videophones [as reported by Rolka Loubé] averages more than one million minutes per month.”²² Yet this measure fails to meaningfully examine the usage data on public and enterprise phones to capture the relative costs and benefits of a log-in requirement.

The Commission cannot lump together the VRS minutes from all enterprise and public videophones, including minutes from enterprise settings such as private offices and shared workspaces or common areas with restricted access, to justify placing log-in requirements. First, imposing login requirements on enterprise videophones, the source of the vast majority of the total public and enterprise VRS minutes reported by Rolka Loubé, would not meaningfully reduce waste, fraud, and abuse. Enterprise videophones are primarily assigned to a specific individual or an area with restricted access. And all enterprise phones are subject to heightened monitoring safeguards. Second, as explained below, the minutes from public phones make up an extremely small proportion of the total number of VRS minutes—far too little to offset the costs to VRS users and providers imposed by the log-in requirement.

²² FNPRM ¶ 61.

The data on record strongly suggest that public phones present no significant risk for fraudulent minute-pumping and the amount of VRS public phone calling continues to decrease. Sorenson previously submitted detailed data on its public and enterprise phones that reveal public phone usage made up just 0.8% of total monthly VRS usage in 2017 and, furthermore, was highly concentrated in the 100 VRS public phones with the greatest VRS usage (which made up nearly half (about 46% on average) of all public phone VRS minutes).²³ From 2017 to 2018, the total number of VRS minutes for Sorenson’s public phones decreased by 10.7%. Public phone usage made up only 0.5% of total VRS usage and was even more highly concentrated in the 100 VRS public phones with the greatest VRS usage, which made up about 60% of all public phone VRS minutes.

Outside the 100 public phones with greatest VRS usage, the average public phone (including those without VRS usage) averaged just *****BEGIN HIGHLY CONFIDENTIAL***** VRS minutes per month in 2018. The number of currently active public phones with any VRS usage in 2018 was *****BEGIN HIGHLY CONFIDENTIAL*****, down 0.8% from 2017.²⁴ In addition, *****BEGIN HIGHLY CONFIDENTIAL***** currently active public phones had only point-to-point and no VRS usage in 2018.

As for enterprise videophones, Sorenson’s data reveal that the average monthly VRS minutes for non-private enterprise phones, where the phone is not assigned to a specific individual but may still be in an area with limited access such as an employee breakroom, was

²³ Sorenson Jan. 26, 2018 Ex Parte at 2-3.

²⁴ The number of public phones with any VRS usage in 2017 was *****BEGIN HIGHLY CONFIDENTIAL*****.

BEGIN HIGHLY CONFIDENTIAL ***END HIGHLY CONFIDENTIAL***

in 2018, down from ***BEGIN HIGHLY CONFIDENTIAL*** ***END HIGHLY CONFIDENTIAL*** average monthly minutes in 2017. The average monthly VRS minutes for private enterprise videophones, where the phone is assigned to a specific individual or is located on a specific individual’s desk, was ***BEGIN HIGHLY CONFIDENTIAL***

END HIGHLY CONFIDENTIAL in 2018, down from ***BEGIN HIGHLY CONFIDENTIAL*** ***END HIGHLY CONFIDENTIAL*** in 2017.

The vast majority of minutes reported by Rolka Loubé,²⁵ therefore, come from enterprise videophones, particularly private enterprise phones assigned to specific individuals. Moreover, for all enterprise videophones, the Commission now requires the enterprise to “make reasonable efforts to ensure that only persons with a hearing or speech disability are permitted to use the phone for VRS.”²⁶ Given the actual use of public phones and safeguards the Commission has already adopted, a log-in requirement for public and enterprise phones would fail to meaningfully reduce waste, fraud, or abuse, and the FNPRM fails to justify imposing costly and burdensome regulatory requirements to reduce a negligible risk.

C. Neustar’s Proposed OAuth Log-in Procedure is Prohibitively Expensive and Technically Infeasible.

The OAuth log-in procedure proposed by Neustar and the FNPRM would impose prohibitive costs on VRS providers and remains technically infeasible for Sorenson’s current public and enterprise videophones. Implementation of the OAuth 2.0 protocol would require VRS devices to have a system web browser, but Sorenson’s ntouch videophones are not

²⁵ *FNPRM* ¶ 61.

²⁶ *Report and Order* ¶ 29.

modifiable to support a system web browser.²⁷ As previously explained, Sorenson designed its ntouch VP1 and VP2 video phones to not include an Internet browser or a keyboard. This design decision enhances security and minimizes risks of device tampering.²⁸ But it renders the ntouch phones unmodifiable to support the proposed log-in mechanism.

Sorenson has researched the memory requirements of all currently available web browsers, including “lightweight browsers.” All exceed the available free memory in the ntouch videophones.²⁹ As a result, if Neustar’s log-in proposal is implemented, Sorenson would have to replace all of its ntouch videophones with a desktop capable of running a web browser and, where that is not operationally or economically feasible, shut down many of the approximately *****BEGIN HIGHLY CONFIDENTIAL***** *****END HIGHLY CONFIDENTIAL***** public phones and *****BEGIN HIGHLY CONFIDENTIAL***** *****END HIGHLY CONFIDENTIAL***** enterprise phones in universities, K-12 schools focused on education of the Deaf, airports, and other institutions with Deaf employees or patrons.

The OAuth implementation costs are staggering. Replacing all of Sorenson’s ntouch videophone with software-based endpoints would cost a total of \$25 million to \$37 million (excluding the costs of modifying software to permit log in). This includes approximately \$2 million to \$3 million for public videophones and \$23 million to \$34 million for enterprise videophones. Moreover, Sorenson would be recovering these costs across a relatively small number of units (its *****BEGIN HIGHLY CONFIDENTIAL***** *****END HIGHLY**

²⁷ Sorenson Nov. 30, 2017 Ex Parte at 2-3.

²⁸ Sorenson Jan. 22, 2018 Ex Parte at 3.

²⁹ Letter from John T. Nakahata, Counsel for Sorenson, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 1 (filed Mar. 5, 2018) (“Sorenson Mar. 5, 2018 Ex Parte”).

CONFIDENTIAL*** public phones and *****BEGIN HIGHLY CONFIDENTIAL*****

*****END HIGHLY CONFIDENTIAL***** enterprise phones), making each unit prohibitively costly. The cost of new desktops with webcams would cost approximately \$1000 per unit and installation would cost approximately \$500 per unit. Sorenson would also incur additional, ongoing maintenance costs to keep the desktops upgraded and to prevent infection from viruses and malware. These devices would also become potential sources of misuse for computer hacking. Additionally, retrofitting the phone booth kiosks custom built for Sorenson’s VP1 and VP2 devices is costly and, in many cases, may not even be possible. The added costs of replacement with a desktop and associated upkeep would lead to shutdown of a significant number of public videophones even if some could be preserved. This would significantly reduce Deaf users’ ability to access VRS services in public and enterprise settings.

Nor do these cost estimates account for the significant costs imposed on other VRS providers. As previously explained, even VRS providers that do not currently deploy any public or enterprise phones still must face the costs to create a server to communicate with the central OAuth server to authenticate users and retrofit their phones to support the OAuth protocol.³⁰

A second method for executing the OAuth 2.0 standard, OAuth 2.0 “Device Flow,” does not require a system web browser for the videophone but is similarly costly and conflicts with functional equivalence. Implementing this device method would cost \$750,000. OAuth 2.0 “Device Flow” requires the user to have access to a secondary device (*e.g.*, a smartphone or computer) to obtain an access token and visit a verification URL to complete the authorization process. However, requiring Deaf users to have an additional device to request and enter an access code, all before they can make or receive a call on a public or enterprise VRS phone, flies

³⁰ Sorenson Jan. 22, 2018 Ex Parte at 4.

in the face of functional equivalence. Hearing users can simply pick up a public or enterprise phone to make or receive calls. Moreover, VRS users that already have access to a smartphone would not need to use a public or enterprise phone when they can easily place or receive VRS calls using providers' smartphone apps. Consequently, the OAuth protocol would render public and enterprise phones "inaccessible to the only users who need them."³¹

Nor is the hypothesized "streamlined version" of OAuth proposed by Neustar a real solution when it, in fact, is not OAuth, is not an industry-accepted authorization protocol standard, and raises serious security and user interface concerns. The "streamlined version" of OAuth alluded to by the FNPRM³² and Neustar³³ is a hypothetical concept that does not meet the OAuth security standard or any widely accepted industry security standard. It is exactly the type of "home-brewed adaptation[]," as critiqued in the studies cited by Sorenson, that expose providers and users to significant security vulnerabilities.³⁴ Under the streamlined approach, the user would enter his or her account name (NANP telephone number) and password on a webpage accessed through a web server where the default VRS provider for the enterprise or public videophone, such as Sorenson, would then pass the user information and password to Neustar (or TRS Numbering Administrator) to provide authorization. There is no system web browser. This approach, however, poses several security risks. For example, it exposes users to man-in-the-middle attacks, where a hacker could inject malware into a public video phone to

³¹ Sorenson Nov. 30, 2017 Ex Parte at 2-3.

³² *FNPRM* ¶ 65.

³³ Letter from Richard L. Fruchterman, III, Senior External Affairs Counsel, Neustar, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 1 ("Neustar Mar. 5, 2018 Ex Parte").

³⁴ *See FNPRM* ¶ 68; Sorenson Mar. 5, 2018 Ex Parte at 1.

collect users’ telephone numbers and passwords. Additionally, without a system web browser, the streamlined approach would provide the default VRS provider for the enterprise or public videophone (in this case, Sorenson) access to the user credentials for other providers, thus defeating the purpose of the OAuth protocol’s security standards.³⁵ Under a full OAuth 2.0 procedure, Sorenson would only have the token granting access to the user, not the user’s actual identity or credentials.³⁶

The streamlined approach’s user interface issue also raises security risks for the customer. The lack of a web browser which enables users to verify the identity of the login server would allow a man-in-the-middle attack. Consumers using the ntouch video phones would need to log in using a remote control and onscreen keyboard, making their credentials vulnerable to identity theft.³⁷ By observing which keys the customer enters on the onscreen keyboard, someone could collect the customer’s password. Providing every public and enterprise video phone with a physical keyboard might be able to decrease this risk, at a greater cost to the provider. But it still fails to safeguard against the security risks where the VRS provider could access the user credentials for other providers. In total, this “streamlined” alternative to OAuth would cost an estimated \$500,000 to implement. While less than the costs of implementing OAuth 2.0, the Commission should not impose a hypothetical, untested log-in procedure that would expose VRS users to significant security risks.

³⁵ Sorenson Jan. 22, 2018 Ex Parte at 3; *see* Sorenson Nov. 30 2017 Ex Parte at 2 n.5 (citing OAuth 2.0 Threat Model and Security Considerations: “[c]lient 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.”).

³⁶ *See FNPRM* ¶ 63.

³⁷ Sorenson Jan. 22, 2018 Ex Parte at 3.

Given the costs, technical challenges, and security risks, the Commission should not impose a log-in requirement using the OAuth standard or its ill-developed alternative. At a minimum, the Commission should exempt unmodifiable ntouch public and enterprise videophones from a log-in requirement. This would save the estimated total of \$25 million to \$37 million implementation costs.

D. Sorenson’s Proposed Alternative Would Impose Less Regulatory and Technical Burdens than the Log-in Requirement, While Still Accomplishing the Commission’s Goal of Fraud Prevention.

Instead of a log-in requirement, the Commission should implement Sorenson’s proposed alternative, which is easily administrable, imposes less burdens on VRS users and providers, and accomplishes the Commission’s goal to reduce waste, fraud, and abuse.³⁸ First, the Commission should implement self-certification of VRS eligibility, which Sorenson already requires for all users before they can use a public videophone for a VRS call.³⁹ Self-certification through a digital signature would not burden Deaf users with having to struggle to remember a passcode or PIN number.⁴⁰ Nor would Deaf users have to provide sensitive personal information to VRS providers to set up or reset their passcode or PIN.⁴¹

Should the Commission want additional controls, it would be sufficient to require a Deaf user to enter his or her VRS phone number, instead of a passcode or PIN, before completing a call. This would allow for the tracking of individual use and permit the TRS Fund Administrator

³⁸ See *FNPRM* ¶ 75.

³⁹ See *id.*; Sorenson May 30, 2017 Comments at 20; Sorenson Mar. 5, 2018 Ex Parte at 2 (explaining Sorenson’s self-certification requirement and language).

⁴⁰ See Consumer Groups Feb. 20, 2018 Ex Parte at 1-2 (explaining burdens of log-in requirement for consumers).

⁴¹ See *id.*

to monitor usage trends at these phones for potential fraud warranting further investigation.⁴²

We caution that requiring users to enter their VRS phone number would still burden VRS users by preventing access for those without a VRS phone number, such as consumers in rural areas or homeless individuals. Sorenson does not support imposing these burdens on VRS users given the extremely low risk for fraud or abuse in public and enterprise videophones. This alternative, however, is significantly less burdensome and exclusionary than the FNPRM’s log-in requirement. Usage monitoring and investigation would allow the Commission to ground its regulations of public and enterprise videophones in data, rather than conjecture.

To clarify the record, Sorenson does not support requiring the person responsible for compliant use of the enterprise or public videophone to self-certify their status as the responsible person on a quarterly basis.⁴³ Although Sorenson had discussed the “possibility” of such a measure, we did not submit it as a proposed alternative.⁴⁴ Requiring VRS providers to track and collect this information from the thousands of responsible persons on a quarterly basis would impose significant burdens on providers and divert resources from more urgent matters such as improving call quality. Instead, the Commission should adopt Sorenson’s proposal that, once a VRS provider has identified the responsible party for the public or enterprise videophone, the

⁴² Sorenson Jan. 22, 2018 Ex Parte at 2; Sorenson Mar. 5, 2018 Ex Parte at 1-2.

⁴³ See *FNPRM* ¶ 76.

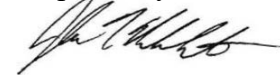
⁴⁴ See Letter from Mark D. Davis, Counsel for Sorenson, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123, at 1 (filed Mar. 25, 2019) (explaining that Sorenson had “discussed the possibility of implementing a quarterly process requiring users of certain enterprise accounts to verify that the account is still being used or supervised by the person or department who it was assigned”).

responsible party bears the obligation to notify the VRS provider of any change in who is the responsible party to monitor that videophone.⁴⁵

CONCLUSION

The Commission should (1) allow VRS providers to provide service to new and porting users for up to two weeks pending the completion of TRS-URD verification and (2) not adopt the proposed log-in requirement for enterprise and public phones. At minimum, the Commission should exempt public and enterprise videophones that are currently in use and cannot be modified to support a system web browser from the log-in requirement.

Respectfully submitted,



John T. Nakahata

Christopher J. Wright

Mark D. Davis

Stephen W. Miller

Mengyu Huang

HARRIS, WILTSHIRE & GRANNIS LLP

1919 M Street, NW, Suite 800

Washington, DC 20036

(202) 730-1300

jnakahata@hwglaw.com

Counsel for Sorenson Communications, LLC

August 5, 2019

⁴⁵ See Sorenson Jan. 26, 2018 Ex Parte at 4 (noting that the Commission could require enterprises requesting videophones to take responsibility for monitoring their use).