

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Structure and Practices of the Video Relay Service) CG Docket No. 10-51
Program)
)
)
)

PETITION FOR DECLARATORY RULING OR WAIVER

Sorenson Communications, Inc. (“Sorenson”) hereby requests a declaratory ruling or waiver regarding the requirements that video relay service (“VRS”) providers route calls through a single uniform resource locator (“URL”), and that providers report each URL through which a call is initiated.¹ Sorenson applauds the Commission’s effort to combat fraud and abuse in the provision of VRS. Indeed, Sorenson agrees with and supports the rationale behind prohibiting providers from allowing end users to place calls using multiple URLs. As the Commission observed in its *Fraud Order* when explaining the need for the rule, providers in the past have generated customer confusion and facilitated fraud by using multiple “public-facing” URLs—to reward individual minute pumpers, to make white-label providers, and for other reasons.² An implausibly strict application of the *Fraud Order*’s single-URL and URL-reporting requirements would cause unintended harm that is entirely divorced from the need to combat fraud and abuse.

¹ See *Structure and Practices of the Video Relay Service Program*, 26 FCC Rcd. 5545, 5574, 5579-80 ¶¶ 57, 73 (2011) (“*Fraud Order*”) (“We... require that calls to any brand or sub-brand of VRS be routed through a single URL address for the brand or sub-brand”; also requiring providers to report “the URL address through which the call was initiated”); see also 47 C.F.R. §§ 64.604(c)(5)(iii)(N)(1)(ii), 64.604(c)(5)(iii)(C)(2)(x) (establishing URL-reporting requirement).

² See *id.* at 5570-71 ¶¶ 48-50.

Thus, in this Petition, Sorenson asks the Commission to issue a declaratory ruling confirming that (1) the single-URL requirement applies only to public-facing URLs that customers may use to place calls, and not to URLs that providers use strictly for redundancy and other back-office functions; and (2) in call detail records (“CDRs”) submitted to the TRS Fund Administrator, VRS providers must report only the URL that a consumer actually uses to initiate sessions (such as dial-around calls), not URLs used for back-office operations, and no URL at all when a customer places calls without knowingly using a URL (which is the case when virtually any VRS user makes a call through his or her default provider’s endpoint, as explained below). This approach reflects the only plausible application of the URL rule.

With respect to the first point presented above—applying the rule only to public-facing URLs—adopting a contrary approach would have debilitating and disruptive consequences for consumers and providers without doing anything to combat waste, fraud or abuse. Simply put, VRS service architecture logically requires providers to employ multiple URLs in their back office operations, even if there is only a single public-facing URL to be used to launch a VRS call. One critical reason for employing more than URL is to ensure system redundancy. For example, in the event that the domain name service (“DNS”) provider supporting a VRS provider’s URL has a system failure (through no fault of the VRS provider), the URL will “go dark” and, under an impractically restrictive reading of the rule, the VRS provider would have no ability to switch over to a back-up DNS provider.³ Under the only practically plausible reading of the rule, however, a provider would be able to employ multiple separate back-office URLs to support system redundancy and facilitate internal call processing (i.e., connecting with hold

³ With a redundant URL infrastructure in place, a provider’s endpoints could “fail over” to the backup URL, and consumers would never know there was an issue. But utilizing this kind of system requires engaging a separate DNS provider for the back-up architecture, which necessarily entails the use of multiple URLs.

servers, accessing advanced features, and call routing). In other words, while a provider may properly be limited to a single *public-facing* URL, a call may validly route through a number of *back-office* URLs that the customer never sees.

Moreover, the use of separate back-office URLs in no way presents any risk of the fraud described in the *Fraud Order*, which pertains entirely to public-facing URLs. But barring providers from using separate back-office URLs would result in severe and completely unnecessary operational disruptions for consumers. The *Fraud Order*'s focus on the possibility for customer confusion (and provider mischief) in the context of branding and URLs indicates clearly that the Commission's directive was aimed at the brands and URLs that consumers see.⁴

With respect to the second point—CDR reporting—the Commission has required that VRS providers' CDRs include “the URL address through which the call was initiated.”⁵ The only plausible understanding of this rule requires that a provider report URL data only when a user initiates a call through a public-facing URL and that the provider report only the public-facing URL the caller used. In other words, the rule cannot practically be understood to require providers to report URL data when a customer does not use a public-facing URL to initiate a call, and a provider need not report any of the back-office URLs that may be utilized during the course of a single call. The reality is that very few VRS calls are initiated through URLs at all. Rather, all (or nearly all) VRS customers using their default providers' endpoints initiate calls simply by picking up the handset or opening the application. In a typical call sequence, the endpoint automatically connects to IP addresses associated with the default provider (typically the same IP addresses to which the public-facing URL would resolve), but without using a URL to do so and certainly without having the customer input any URL. Providers *could* insert their

⁴ See *Fraud Order* at 5570-71 ¶¶ 48-50.

⁵ *Id.* at 5579-80 ¶ 73; see also 47 C.F.R. § 64.604(c)(5)(iii)(C)(2)(x).

public-facing URL address on their CDRs even for these calls (on the theory that their URLs resolve to the same IP addresses as non-URL-initiated calls from default customers), but that would provide no meaningful information related to the call—and certainly no information related to detecting waste, fraud or abuse. For this reason, the rule should be understood to require providers to supply URL data on their CDRs only when VRS users employ a URL to initiate a call, and to leave that data field empty in other cases.⁶

For the same reason, the rule should be understood to require providers to report only the public-facing URL through which a call routes, and not any back-office URLs employed for redundancy and other back-office operational purposes. Requiring providers to submit back-office URL data would do nothing to combat waste, fraud and abuse, but it would introduce needless burden and expense into the reporting process while rendering CDRs a cumbersome mess for RLSA. It does not serve the public interest to force providers to needlessly devote resources to tracking and reporting information that does not help the Commission identify fraud. If anything, requiring the submission of this data would hamper fraud-prevention goals as the Commission and TRS Fund Administrator would need to sift through irrelevant data associated in an effort to identify unscrupulous practices.

For all of these reasons, Sorenson requests that the Commission issue a declaratory ruling confirming that (1) the URL rule applies only to public-facing URLs that customers use to place calls, and not to URLs that are used strictly for redundancy and back-office functions; and (2) in their CDRs filed with the TRS Fund Administrator, VRS providers must report only the URL that a consumer actually uses to initiate sessions, and no URL at all when a customer places calls without employing a URL at all.

⁶ Rolka Loubé Saltzer Associates (“RLSA”) has informally advised that this field should be left empty in cases where users do not employ a URL to initiate a call.

Should the Commission disagree that this is the proper understanding of the rule, Sorenson requests a waiver authorizing the approach described above. The Commission may waive its rules when there is “good cause” to do so.⁷ Waiver is appropriate if circumstances warrant a deviation from the general rule, and such deviation would better serve the public interest than would strict adherence to the general rule.⁸ For the reasons presented above, there is good cause to issue a waiver in this circumstance if the Commission disagrees with the interpretation of the rule presented above.

Respectfully submitted,

/s/ John T. Nakahata

John T. Nakahata
Christopher J. Wright
Charles D. Breckinridge
Walter E. Anderson
WILTSHIRE & GRANNIS LLP
1200 Eighteenth Street, N.W.
Washington, D.C. 20036
T: (202) 730-1300
jnakahata@wiltshiregrannis.com

Counsel to Sorenson Communications, Inc.

Michael D. Maddix
Director of Government and
Regulatory Affairs
SORENSEN COMMUNICATIONS, INC.
4192 South Riverboat Road
Salt Lake City, UT 84123

December 22, 2012

⁷ 47 C.F.R. § 1.3.

⁸ *Ne. Cellular Tel. Co., L.P. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990) (citing *WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969)).