

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In The Matter of)	
)	
Misuse of Internet Protocol Relay Service)	CG Docket No. 12-38
)	
)	
Telecommunications Relay Services and Speech- to-Speech Services for Individuals with Hearing and Speech Disabilities)	CG Docket No. 03-123
)	

COMMENTS OF SORENSON COMMUNICATIONS, INC.

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

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

Counsel to Sorenson Communications, Inc.

March 20, 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
I. ILLEGITIMATE IP RELAY CALLS STRAIN THE TRS FUND AND HARM THE INTEREST OF <i>BONA FIDE</i> USERS	1
II. THE CURRENT VERIFICATION SYSTEM IDENTIFIES LEGITIMATE USERS, BUT IT REMAINS VULNERABLE TO FRAUD BECAUSE PROVIDERS MUST OFFER SERVICE EVEN BEFORE VERIFICATION IS COMPLETE	2
A. Sorenson’s IP Relay Verification System Works	3
B. The Commission Should Eliminate Users’ Ability to Make Calls Prior to Registration Verification	4
III. THE COMMISSION SHOULD ALSO CONSIDER MEASURES TO IDENTIFY FRAUDULENT CALLS ON A CASE-BY-CASE BASIS	6
A. IP Relay Providers Can Identify Many Fraudulent Calls Based on a Call-by-Call Assessment	6
B. IP Relay Providers Cannot Identify Calls From Overseas When the Caller Masks the IP Address	8
C. IP Relay Providers Should be Required to Retain Records Pertaining to Illegitimate Calls	8
D. IP Relay Users Do Not Use Dial-Around	9
E. If the Commission Bars Interim IP Relay Calling Pending Verification, There Will Be No Need to Share Lists of Blocked Callers	9
F. IP Relay Provides a Valuable Communications Option Unavailable Via Other Forms of TRS	10
IV. CGB SHOULD ADDRESS ADDITIONAL MODIFICATIONS TO IP RELAY BEYOND THOSE COVERED IN THE PUBLIC NOTICE	12
A. Providers Should Report on a Quarterly Basis the Aggregate Percentage of IP Relay Calls Involving Credit Cards	12
B. Work-Related Calls To or From TRS Providers’ Employees Should Not Be Compensable	13
V. CONCLUSION	14

EXECUTIVE SUMMARY

Sorenson Communications, Inc. (“Sorenson”) files these comments in response to the Public Notice issued by the Consumer and Governmental Affairs Bureau (“CGB” or “the Bureau”), seeking to “refresh the record on several issues pertaining to misuse of Internet Protocol (IP) Relay Service.”¹ Sorenson concurs with CGB that IP Relay service continues to be disproportionately susceptible to fraud for many providers, and Sorenson therefore commends the Bureau for taking steps to address the problem.

As explained below, there are several measures through which the Federal Communications Commission (“FCC” or “Commission”) could virtually eliminate misuse of IP Relay almost immediately. First, and most importantly, the Commission should stop requiring providers to allow users to make IP Relay calls before their eligibility has been verified. In Sorenson’s experience, virtually all IP Relay misuse is attributable to users who have not been verified, so closing this loophole would resolve the problem almost immediately.

Second, the Commission could implement rules requiring IP Relay communications assistants (“CAs”) to monitor the calls they handle for certain indications of misuse. In the event a CA identified any such indications in a particular call, and if the CA’s supervisor agreed that there were indications of misuse, the CA would alert the hearing party of the issue (using a dedicated script) and would offer to terminate the call. Sorenson has already implemented this kind of procedure in its own IP Relay service, and it believes that it has largely eradicated misuse of the service.

Third, CGB or the Commission should require providers to maintain and periodically report aggregated (but not user-identifiable) data on the proportion of IP Relay calls that involve

¹ *Consumer & Governmental Affairs Bureau Seeks to Refresh the Record Regarding Misuse of Internet Protocol Relay Service*, Public Notice at 1, CG Docket Nos. 12-38 & 03-123 (rel. Feb. 13, 2012) (“Public Notice”).

a credit card in any way. While this would not affect callers' privacy interests (because the data would be maintained only in aggregate), it would enable the Commission to identify and investigate situations in which the percentage is outside of the industry norm.

Finally, CGB or the Commission should clarify that the prohibition against compensating employees' calls applies to all forms of Telecommunications Relay Service ("TRS"), not just Video Relay Service ("VRS").

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In The Matter of)	
)	
Misuse of Internet Protocol Relay Service)	CG Docket No. 12-38
)	
)	
Telecommunications Relay Services and Speech- to-Speech Services for Individuals with Hearing and Speech Disabilities)	CG Docket No. 03-123
)	

COMMENTS OF SORENSON COMMUNICATIONS, INC.

For the reasons set forth below, Sorenson urges CGB or the Commission to eliminate the rule allowing IP Relay users to make calls before verifying their registrations. In addition, assessing the legitimacy of IP Relay calls on a case-by-case basis can effectively combat fraud, but not as reliably as closing the pre-verification calling ability described above. Sorenson also urges the Commission to require providers to submit data on a periodic basis identifying the proportion of IP Relay calls involving a credit card, as an additional tool for identifying patterns or providers that require a closer look. Finally, Sorenson recommends expressly extending to all forms of TRS the current rule barring compensation for work-related calls to or from providers' employees.

I. ILLEGITIMATE IP RELAY CALLS STRAIN THE TRS FUND AND HARM THE INTEREST OF *BONA FIDE* USERS

Misuse of IP Relay generates a variety of problems. At the most fundamental level, of course, it places an unnecessary and illegitimate strain on the TRS Fund and on the telecommunications end users whose obligatory contributions fund it. Fraudulent IP Relay calls also harm the interests of legitimate IP Relay users because merchants, after exposure to

fraudulent calls, may be reluctant to engage in any transactions via IP Relay. This reluctance degrades the utility of IP Relay for deaf, hard-of-hearing and speech-disabled users, even though it is the most functionally equivalent form of text-based TRS that is currently available. IP Relay fraud harms providers as well. The perpetrators of IP Relay fraud have proven to be resourceful and adaptive, and they continually modulate the patterns of their schemes to avoid detection. The resulting lack of predictability compels providers to increase staffing of IP Relay CAs to ensure they can respond to spikes in call volume that may be caused by fraudulent calls while still meeting the speed-of-answer requirements. Needless to say, this overstaffing decreases providers' efficiency and increases their costs.

Sorenson is encouraged by the release of CGB's Public Notice, as it demonstrates that CGB and the Commission are aware of the problem and developing a process to address it. Unless CGB and the Commission take decisive action to combat IP Relay misuse, the service will become less and less useful for consumers, including both the hearing and speech disabled as well as the general public. That outcome would directly contravene the Americans with Disabilities Act ("ADA"), which requires the Commission to "ensure" that IP Relay (and all other forms of TRS) are "available, to the extent possible" to all deaf, hard-of-hearing, and speech-disabled individuals.² The Commission must therefore act swiftly to curb the fraudulent use of IP Relay.

II. THE CURRENT VERIFICATION SYSTEM IDENTIFIES LEGITIMATE USERS, BUT IT REMAINS VULNERABLE TO FRAUD BECAUSE PROVIDERS MUST OFFER SERVICE EVEN BEFORE VERIFICATION IS COMPLETE

Sorenson has found that its current verification system successfully identifies legitimate and eligible IP Relay users; indeed, to its knowledge, Sorenson has experienced virtually no

² 47 U.S.C. § 225(b)(1).

misuse of IP Relay at the hands of users who have been verified. The IP Relay system is still vulnerable to fraud, however, because of the requirement that providers grant temporary authorization to users even before the verification process is complete. Eliminating users' temporary calling capability would eliminate IP Relay misuse almost immediately.

A. Sorenson's IP Relay Verification System Works

CGB inquires in the Public Notice whether the existing verification system for IP Relay is effective.³ In Sorenson's case, the answer is yes—although, as noted in the following subsection, there is a more systemic vulnerability, as the FCC's rules require providers to process IP Relay calls even while a user's verification is pending.

While IP Relay users can register online, Sorenson uses a paper-based process to verify them. To register for Sorenson's IP Relay service, a user must supply Sorenson with his or her name and a valid U.S. mailing address. Immediately after a new user registers, Sorenson sends a verification letter to the address the new user provided. In accordance with the FCC's IP Relay verification requirements,⁴ the letter requires the user to send a response to Sorenson including the following: (a) verification of the user's name; (b) a self-certification that the user is substantively eligible (that is, that he or she has hearing loss or a speech disability); and (c) a copy of documentation (such as a utility bill) that confirms the user's address. While the Commission has never set a deadline by which users must respond to verification efforts, Sorenson terminates service for any user who fails to respond to the verification request within six months of registering.

³ See Public Notice at 5-6.

⁴ See *Telecommunications Relay Services & Speech-to-Speech Services for Individuals with Hearing & Speech Disabilities*, Second Report and Order and Order on Reconsideration, 24 FCC Rcd. 791, 809-10 ¶¶ 37-38 (2008) (“December 2008 Numbering Order”).

The verification process works when it is allowed to run its course—Sorenson users who have successfully verified their registrations are not a source of fraudulent IP Relay calls. There is therefore no need to impose additional documentation requirements or to mandate revalidation of already verified IP Relay users in order to combat fraud.⁵ Instead, the Commission should eliminate callers' ability to use the service before verification is complete.

B. The Commission Should Eliminate Users' Ability to Make Calls Prior to Registration Verification

IP Relay's vulnerability to fraud arises from the requirement that providers allow users to make IP Relay calls even before the verification process is complete. Eliminating that requirement would eliminate IP Relay misuse almost immediately. In Sorenson's experience, fraudulent IP Relay users do not complete the verification process. They rely instead on the interim authorization to make calls, as required under the rules. And once they can no longer make IP Relay calls via one particular temporary authorization, they simply re-register under another assumed name and start the process over again.

When it established a system for TRS providers to assign users of VRS and IP Relay ten-digit telephone numbers linked to the North American Numbering Plan, the Commission recognized that "requiring Internet-based TRS providers to offer their users a means of registering will help reduce the abuse of IP Relay for fraudulent purposes."⁶ The Commission therefore concluded that "[t]o verify the accuracy of initial registration information and to help ensure that VRS and IP Relay are used only for their intended purpose, . . . Internet-based TRS providers must institute procedures to verify the accuracy of registration information, including

⁵ See Public Notice at 6 (asking whether the Commission should adopt additional documentation requirements and require revalidation of verified IP Relay users).

⁶ *Telecommunications Relay Services & Speech-to-Speech Services for Individuals with Hearing & Speech Disabilities*, Report and Order and Further Notice of Proposed Rulemaking, 23 FCC Rcd. 11,591, 11,632 ¶ 118 (2008) ("June 2008 Numbering Order").

the consumer's name and mailing address, before issuing the consumer a ten-digit telephone number.”⁷ At the same time, however, the Commission “conclude[d] that to the extent technically feasible, Internet-based TRS providers must allow newly registered users to place calls immediately”⁸—that is, even before the verification process is complete.

In a subsequent public notice, CGB “emphasize[d] that . . . provider[s] must handle calls to or from [registered, yet unverified] callers, to the extent technically feasible, even if the provider has not completed verifying that information, assigning the caller a new ten-digit number, and provisioning that number to the iTRS database.”⁹ CGB further clarified that “[t]o the extent . . . the Numbering Order & FNPRM suggests that the provider must provide the caller with a ten-digit number before handling any calls for that consumer, we clarify that, as set forth more specifically in the Second Numbering Order, VRS and IP Relay providers must allow newly registered users to place calls immediately after they have submitted all of the necessary registration information.”¹⁰

The requirement to enable IP Relay users to make calls before their verification is complete creates a loophole that enables virtually every fraudulent IP Relay call. Sorenson urges CGB and the Commission to close the loophole immediately by removing the requirement. While verification remains outstanding, the IP Relay provider should be required to process a user's emergency calls but no others.

⁷ *December 2008 Numbering Order*, 24 FCC Rcd. at 809 ¶ 37.

⁸ *Id.* at 803 ¶ 25.

⁹ *Consumer & Governmental Affairs Bureau Reminds Video Relay Service (VRS) & Internet Protocol (IP) Relay Service Providers of Their Outreach Obligations & Clarifies Their Call Handling Obligations for Unregistered Users After the November 12, 2009, Ten-Digit Numbering Registration Deadline*, Public Notice, 24 FCC Rcd. 12,877, 12,879 (2009).

¹⁰ *Id.* at 12,879 n.14 (internal citations and emphasis omitted).

While this change would be devastating for illegitimate IP Relay users, the impact on valid customers would be modest. Under Sorenson's verification system, for instance, a legitimate IP Relay user could obtain active service in a matter of days by responding promptly to Sorenson's verification letter. Even this modest impact would affect only a small number of future IP Relay users because, as explained above, there would be no reason to re-verify customers who have already successfully completed the verification process. And the number of future IP Relay users experiencing any substantial, real-world impact will be still smaller, because many will likely have access to other forms of TRS during the interim period.

III. THE COMMISSION SHOULD ALSO CONSIDER MEASURES TO IDENTIFY FRAUDULENT CALLS ON A CASE-BY-CASE BASIS

CGB's Public Notice poses additional questions related to identifying illegitimate calls on a case-by-case basis. As explained below, Sorenson believes that there are effective techniques for flagging and identifying problematic calls as they occur. But none of these techniques would be as effective as simply eliminating callers' ability to use IP Relay while their verifications remain pending.

A. IP Relay Providers Can Identify Many Fraudulent Calls Based on a Call-by-Call Assessment

While eliminating interim calling pending verification would provide the most thorough and objective means of combating IP Relay fraud, call-by-call assessments can present a strong defense as well.¹¹ In fact, because of the apparently fraudulent calls that it receives from unverified users, Sorenson has implemented a procedure of this kind already, and it has proved to be highly effective.

¹¹ See Public Notice at 6-7 & n.36.

Sorenson’s process for identifying illegitimate calls depends on a list, developed by Sorenson, that identifies twelve separate indications that a call may be illegitimate.¹² (Sorenson does not make the list public because that would give fraudulent callers a roadmap for bypassing the controls.) Sorenson directs its IP Relay CAs to be on the alert for any of the call characteristics on the list. If a CA determines that a particular call meets at least two of the twelve indicators, the CA notifies his or her supervisor. If the supervisor agrees that at least two of the indicators are present, the CA reads a script to the hearing end user warning that the call may be illegitimate and offers to terminate it.

This process does not appear to have negatively affected any valid IP Relay calls: Sorenson has not received a single complaint—from an IP Relay subscriber or from the hearing end user on an IP Relay call—that this system has impeded any legitimate communication. But the impact on suspect calls has been dramatic. While a meaningful percentage of Sorenson’s IP Relay calls involved some form of potentially fraudulent financial transactions when Sorenson first began offering the service, that figure has precipitously dropped to less than one percent as a result of the fraud prevention measures Sorenson has adopted – and those that remain are conducted after notice to the recipient of the suspect IP Relay communication.¹³

If the Commission does not eliminate the pre-verification call-handling requirement, adopting a call-by-call assessment obligation could help reduce the volume of industry-wide IP Relay fraud, as it already has for Sorenson. This approach suffers from two key weaknesses, however. First, it depends on CAs’ attention and is therefore subject to human error. If CAs are

¹² Additionally, Sorenson has developed a list of nineteen different indicators which require that only one indicator be met before the CA alerts a supervisor and, upon the supervisor’s approval, alerts the hearing partying.

¹³ Sorenson has been, and remains, cognizant of its primary role to serve as a functionally equivalent “dial tone” for legitimate TRS users, but also recognizes its role in vigilantly guarding against fraudulent TRS use.

not consistently vigilant, then fraud will persist. Second, adopting this kind of system industry wide would increase the risk that someone would leak the list of fraud indicators. If the list were to fall into the hands of the perpetrators of IP Relay fraud, they would be able to adapt their schemes to subvert the controls.

B. IP Relay Providers Cannot Identify Calls From Overseas When the Caller Masks the IP Address

CGB's Public Notice asks further whether IP Relay providers have tracking mechanisms or other techniques available to identify calls that originate abroad even when the overseas caller masks his or her IP address.¹⁴ The answer is no. If an IP Relay caller based overseas takes steps to mask the originating IP address or spoof a U.S. IP address, Sorenson cannot identify it as a foreign-origin call.

C. IP Relay Providers Should be Required to Retain Records Pertaining to Illegitimate Calls

In response to CGB's inquiry related to record retention,¹⁵ Sorenson recommends that the Commission require IP Relay providers to keep limited records of calls that the provider has determined to be illegitimate. As CGB suggests, preserving these records and, when appropriate, submitting them to the Commission would assist in TRS program oversight. In particular, keeping such records would help improve processes for recognizing fraudulent calls; enable the Commission to identify and work with providers that appear to have difficulty flagging improper calls; identify individual CAs who may need further training or guidance with respect to problematic calls; and create a record that could help recreate events if a caller later disputes the provider's view that the call was illegitimate.

¹⁴ *See id.* at 7.

¹⁵ *See id.*

Moreover, this record-keeping requirement would not violate the ADA's confidentiality protections or the FCC's existing regulations barring the retention of call-content records. The protections in the existing rules apply only to TRS calls. But, by definition, the illegitimate calls for which providers would retain records do *not* constitute legitimate TRS calls, and accordingly the standard protections do not apply.

D. IP Relay Users Do Not Use Dial-Around

CGB asks further whether callers use dial-around options with IP Relay.¹⁶ In Sorenson's experience, they do not. It appears that IP Relay users often have accounts with multiple providers' services at the same time, so they have no need to dial around. Instead, they just place each IP Relay call via the service they want to use.

E. If the Commission Bars Interim IP Relay Calling Pending Verification, There Will Be No Need to Share Lists of Blocked Callers

At present, Sorenson maintains a list of IP Relay users whose accounts Sorenson has blocked because of past fraudulent calls.¹⁷ Rather than keep a list of blocked ten-digit numbers, Sorenson maintains a list of blocked screen names, which Sorenson finds to be an easier way to identify most IP Relay callers. (Approximately ninety percent of IP Relay calls are placed over GoogleTalk or AOL Instant Messenger ("AIM"), both of which identify callers by screen name.) Sorenson does not permit future IP Relay calls from screen names included on its list.

Sorenson does not share the list with other IP Relay providers, and it is not aware of any other providers that make comparable lists available to competitors. Moreover, Sorenson does not believe that the FCC should obligate providers to share their lists—with each other or with a centralized clearinghouse of blocked accounts. Indeed, if the Commission eliminates interim IP

¹⁶ See *id.* at 7-8.

¹⁷ See *id.* at 8 (inquiring whether providers keep lists of blocked callers, and whether they should be required to share them with each other or with a central database).

Relay calling pending user verification, there would effectively be no need to keep or share such lists in any event. Conversely, if the Commission does not eliminate interim IP calling, sharing blocked caller lists would be ineffective, since perpetrators of IP Relay fraud could continue their current approach of frequent identity changes to take advantage of the interim loophole. As discussed above, there is nothing to prevent fraudsters from signing up for interim IP Relay service using a new number or screen name once illegitimate calls are discovered, so the previously-used identification is likely to have been discarded by the time it has been added to the list. Moreover, unless the lists are shared in real-time—which would be difficult to administer—alerting other providers to particular fraudulent identities is likely to come too late to be useful. Finally, sharing lists would increase the risk that some provider would erroneously identify a legitimate number or screen name as fraudulent, thus excluding that legitimate user from any service provider. Instead of list sharing, providers should adopt robust safeguards to root out IP Relay fraud and effectively deter fraudsters from using this important service for illicit means.

F. IP Relay Provides a Valuable Communications Option Unavailable Via Other Forms of TRS

The Public Notice asks further whether IP Relay is widely used by consumers and whether other forms of TRS provide an adequate alternative—questions that suggest the Bureau is considering whether there is reason to continue supporting IP Relay at all in light of the fraud it has enabled.¹⁸ Even though Sorenson’s IP Relay call volumes are relatively small in comparison to VRS, Sorenson firmly refutes any suggestion that IP Relay should be eliminated as a compensable form of TRS.

¹⁸ *See id.*

First, as discussed above, fraud should not be a consideration in eliminating IP Relay. The fraud that has tarnished the service can be eliminated almost immediately—by barring callers from using the service before verification is complete. Even more fundamentally, however, *bona fide* consumers value IP Relay because it enables legitimate relay communications in contexts that other forms of TRS simply cannot replicate. Mobile communications provide a useful example. While many mobile devices are not suitable for VRS communications, IP Relay remains a viable option.

Secondly, preserving IP Relay is vital because of its potential to serve as a text-to-911 solution for the deaf and hard-of-hearing. Unlike SMS, IP Relay offers deaf and hard-of-hearing individuals a reliable and established way to reach 911 through flexible and readily-available CAs. Through a series of Orders the Commission has mandated that a handset capable of operating the IM client used by an IP Relay provider must allow a user to connect to 911. IP Relay providers are required “transmit all 911 and E911 calls, as well as a call back number, the name of the relay provider, the CA’s identification number, and the caller’s Registered Location for each call, to the PSAP.”¹⁹

Indeed, commenters in other proceedings have noted the importance of IP Relay as a text-to-911 solution. The Alliance for Telecommunications Industry Solutions (“ATIS”) Interim Non-Voice Emergency Services (“INES”) Report and Recommendations concluded: “From a technical perspective, IP Relay is the best alternative for interim [text-based] emergency

¹⁹ *Telecommunications Relay Services & Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; E911 Requirements for IP-Enabled Service Providers*, 23 FCC Rcd. 11,591, 11,620 ¶ 82 (2008). See also 47 C.F.R. § 64.605 (emergency call handling requirements for IP Relay and VRS).

communications” by the Commission’s 2012 target timeframe.²⁰ The ATIS INES Report and Recommendation specifically described the features of IP Relay that make it the most promising near-term text to 911 solution.²¹ In short, IP Relay remains an effective and vital avenue for deaf and hard of hearing individuals to reach critical emergency assistance. Sorenson accordingly urges CGB to recognize the unique service that IP Relay provides to verified and legitimate end users, and to maintain IP Relay as a compensable form of TRS.

IV. CGB SHOULD ADDRESS ADDITIONAL MODIFICATIONS TO IP RELAY BEYOND THOSE COVERED IN THE PUBLIC NOTICE

In addition to the issues covered in the Public Notice, the Bureau should also consider two additional issues when assessing IP Relay reform. First, as a tool for identifying patterns of fraudulent conduct, it should consider requiring providers to collect aggregated data on the proportion of IP Relay calls that involve the use of a credit card. Second, to combat waste, fraud and abuse, it should clarify that any work-related TRS call to or from a provider’s employee is not a compensable call.

A. Providers Should Report on a Quarterly Basis the Aggregate Percentage of IP Relay Calls Involving Credit Cards

The Commission has recognized that credit card misuse is a particular source of IP Relay fraud. In one of the most common forms of IP Relay misuse, people without any hearing loss or speech disability use IP Relay services to defraud merchants by making purchases over the

²⁰ *Comments of the Alliance for Telecommunications Industry Solutions* at exec. sum. 2, PS Docket Nos. 11-153 & 10-255 (filed Dec. 12, 2011).

²¹ *Id.* at 17. “IP Relay is available currently to anyone who has access to the Internet via a computer, personal digital assistant (PDA), Web-capable telephone, or other device; IP Relay applications are available for popular mobile device operating systems, as well as IM applications; IP Relay allows consumers to make emergency calls without having to purchase, carry, and connect TTY equipment; IP Relay allows bidirectional text communications with the CA; Transmission quality may be faster via IP Relay than via a TTY; Some IP Relay services also support other media besides text such as video or voice.”

telephone using stolen, fake, or otherwise invalid credit cards.²² To help address this distinct form of IP Relay fraud, Sorenson suggests that the Commission require providers to monitor and report on credit card usage on an aggregated basis. In particular, providers should be required to file quarterly reports with the Commission and the TRS Fund Administrator identifying the proportion of IP Relay calls they handled in the preceding quarter that involved a credit card or credit card number in any way. Such a requirement would help providers and the Commission identify spikes that might indicate fraud and that therefore merit a closer look. This requirement would also alert the Commission to IP Relay providers that may not have instituted sufficient internal controls to prevent IP Relay misuse and fraud. By collecting such data only on an aggregated basis, however, this requirement would anonymize the resulting information and therefore would not impact users' privacy rights.

B. Work-Related Calls To or From TRS Providers' Employees Should Not Be Compensable

Sorenson further proposes that CGB (or the Commission as a whole) combat waste, fraud and abuse by clarifying that all workplace and work-related TRS communications made by or to employees of any TRS provider are not compensable from the TRS Fund. In February 2010, CGB issued a Declaratory Ruling holding that work-related VRS calls made by or to an employee of a VRS provider are not eligible for compensation.²³ Instead of compensating those calls on a per-minute basis, CGB required that costs associated with those calls be considered business expenses and submitted to the TRS Fund Administrator for consideration in calculating

²² See *June 2008 Numbering Order*, 23 FCC Rcd. at 11,624 ¶ 92; see also *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, Further Notice of Proposed Rulemaking, 21 FCC Rcd. 5478, 5483 ¶¶ 11, 13 (2008).

²³ *Structure and Practices of the Video Relay Service Program*, Declaratory Ruling, 25 FCC Rcd. 1868 (2010).

the VRS compensation rate. CGB reasoned that employee calls are business expenses that a provider must bear to accommodate employees who require relay service, just as any employer must bear the cost of providing phone service to employees who do not have hearing loss or a speech disability.²⁴

As CGB acknowledged, the principles it articulated the Declaratory Ruling are applicable to all forms of TRS providers' employee communications.²⁵ Accordingly, Sorenson does not seek compensation from the Fund for any of its employees' work-related TRS communications. Reflecting its own approach and the underlying rationale of the Declaratory Ruling, Sorenson urges CGB or the Commission to clarify that the prohibition on compensation for work-related employee communications extends to all forms of TRS.

V. CONCLUSION

For the foregoing reasons, Sorenson urges CGB or the Commission to eliminate the rule allowing IP Relay users to make calls before verifying their registrations. Additionally, Sorenson recommends that CGB or the Commission take additional steps to combat fraud, waste and abuse of the TRS Fund.

²⁴ The phrases "employee calls" and "employee communications" should be understood to mean workplace or work-related calls. This reflects CGB's reasoning that employee calls unrelated to work and made outside of the workplace are compensable. *See id.* at 1870 ¶ 5 n.13.

²⁵ *Id.* at 1869 ¶ 2 n.5 ("Notwithstanding the release of this Declaratory Ruling in a new docket specifically relating to VRS, the principles enunciated in this Declaratory Ruling pertain to all forms of TRS.").

Respectfully submitted,

/s/

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

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

Counsel to Sorenson Communications, Inc.

March 20, 2012