

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

In the Matter of)	
)	
Telecommunications Relay Services and)	
Speech-to-Speech Services for)	CG Docket No. 03-123
Individuals with Hearing and Speech)	
Disabilities)	
)	
Misuse of Internet Protocol (IP) Relay)	
Service and Video Relay Service)	

COMMENTS OF SORENSON COMMUNICATIONS, INC.

Michael D. Maddix
Product Manager
Sorenson Communications, Inc.
4393 South Riverboat Road
Suite 300
Salt Lake City, Utah 84123

Gil M. Strobel
Richard D. Mallen
Lawler, Metzger, Milkman & Keeney, LLC
2001 K Street NW, Suite 802
Washington, DC 20006
(202) 777-7700
gstrobel@lmmk.com

Counsel to Sorenson Communications, Inc.

July 3, 2006

Table of Contents

I.	INTRODUCTION AND SUMMARY	1
II.	DISCUSSION	4
A.	IP Relay Fraud Is a Serious Problem that Requires FCC Action.....	4
B.	The FCC Should Require Providers to Take Appropriate Actions to Reduce IP Relay Fraud.....	5
C.	Other Approaches Would Not Be Effective	9
D.	Sorenson’s Proposed Solution Would Be Legally Sound.....	10
E.	The FCC Should Authorize CAs and Interpreters to Terminate Any TRS Call that Is Obviously Illegitimate	12
III.	CONCLUSION.....	14

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

In the Matter of)	
)	
Telecommunications Relay Services and)	
Speech-to-Speech Services for)	CG Docket No. 03-123
Individuals with Hearing and Speech)	
Disabilities)	
)	
Misuse of Internet Protocol (IP) Relay)	
Service and Video Relay Service)	

COMMENTS OF SORENSON COMMUNICATIONS, INC.

Sorenson Communications, Inc. (“Sorenson”) submits these Comments in response to the Further Notice of Proposed Rulemaking (“*Further Notice*”)¹ released in the above-captioned proceeding, in which the Federal Communications Commission (“Commission” or “FCC”) seeks comment on how to curtail the misuse of the two Internet-based forms of telecommunications relay service (“TRS”), Internet Protocol (“IP”) Relay Service and Video Relay Service (“VRS”).

I. INTRODUCTION AND SUMMARY

IP Relay is the most functionally equivalent form of text-based TRS available today. Increasingly, however, the usefulness of IP Relay is threatened by a serious problem: the fraudulent use of the service, typically by a person located outside the

¹ *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities, Misuse of Internet Protocol (IP) Relay Service and Video Relay Service*, Further Notice of Proposed Rulemaking, 21 FCC Rcd 5478 (rel. May 8, 2006) (FCC 06-58) (“*Further Notice*”).

United States who places an IP Relay call to a U.S. merchant, and then uses a stolen or fake credit card to order merchandise to be shipped outside the United States.²

Unless the Commission acts to address this problem, merchants will become less and less willing to accept IP Relay calls, and, as a result, deaf, hard-of-hearing, and speech-disabled Americans will no longer be able to rely on IP Relay as a means of conducting important transactions in their day-to-day lives. Under the Americans with Disabilities Act (“ADA”), the Commission is required to ensure that this outcome does not in fact occur.³

The need to curb the fraudulent use of IP Relay is particularly acute because of the extent to which the service already has, in the four years it has been available, enhanced the quality of life of deaf, hard-of-hearing, and speech-disabled Americans. Prior to the recognition of IP Relay as a form of TRS in 2002, users were effectively tethered to text telephones (“TTYs”), specialized devices connected via a dedicated link to the Public Switched Telephone Network (“PSTN”). With the advent of IP Relay, users were freed to make a text-based relay call via the Internet using a computer, web phone, personal digital assistant, or many other IP-capable devices, rather than only a dedicated TTY.⁴ By harnessing the versatility, power, and ubiquity of the Internet, IP Relay has been able to provide users substantial benefits – “in quality and flexibility of service, in ease of use and convenience, and in the potential for additional service features in the

² *Id.* ¶ 6.

³ 47 U.S.C. § 225(b)(1).

⁴ *Further Notice* ¶ 5.

future” – that could not be achieved with traditional TTY-based service.⁵ As a result, thousands of deaf, hard-of-hearing, and speech-disabled Americans have come to rely on IP Relay, and many more no doubt will do so – provided the integrity of the service remains intact.

Sorenson has sought to prevent the fraudulent use of IP Relay from jeopardizing this important service. As explained below, Sorenson already has begun to address this problem and protect the interests of legitimate users. However, the Commission needs to take a more active role to ensure a uniform, industry-wide response to this problem.

Any solution mandated by the Commission should achieve two key goals. First, the solution should afford providers the flexibility to adapt to the ever-changing tactics used by the perpetrators of fraud. Second, the solution should be narrowly tailored to address the problem, while still complying with relevant statutes and protecting legitimate users. The Commission could achieve these goals by requiring providers to (i) block international IP Relay calls; and (ii) flag any non-blocked call that meets certain specified indicia of fraud. The Commission also should authorize Communications Assistants (“CAs”) and interpreters to terminate any call that is obviously not a legitimate TRS call.

⁵ *Provision of Improved Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 17 FCC Rcd 7779, ¶ 7 (2002) (summarizing record evidence of benefits of IP Relay); *see also* “IP Relay Service: FCC Consumer Facts,” *available at*: <<http://www.fcc.gov/cgb/consumerfacts/iprelay.html>> (listing the following benefits of IP Relay: availability, convenience, multiple calls, quality, and multivendoring).

II. DISCUSSION

A. IP Relay Fraud Is a Serious Problem that Requires FCC Action

The various benefits of IP Relay have made it a popular means for deaf, hard-of-hearing, and speech-disabled users to access the telephone system and communicate with hearing individuals. Every day, numerous IP Relay calls are made by legitimate users for legitimate purposes.

As the *Further Notice*, news reports, and private parties have documented, however, IP Relay increasingly has been misused by persons without a hearing or speech disability to defraud merchants.⁶ A large portion of these fraudulent calls are placed by persons outside the United States to a business within the United States, typically using a stolen or fraudulent credit card to order goods to be shipped to a foreign location.⁷

Such misuse of IP Relay is problematic for a variety of reasons. For instance, the misuse harms legitimate users because they may no longer be able to convince merchants to accept their orders for merchandise.⁸ Such inability, in turn, artificially constrains the use of IP Relay, even though it is the most functionally equivalent form of text-based TRS that is currently available. Furthermore, the perpetrators of fraud have proven to be resourceful and adaptive, and continually modulate the patterns of their schemes to avoid detection. The resulting lack of predictability compels providers to increase staffing of CAs to respond to unexpected spikes in call activity that may be caused by fraudulent

⁶ See *Further Notice* ¶ 6 & n.25.

⁷ *Id.* ¶ 6.

⁸ See, e.g., *id.* ¶ 7; Letter from Ray H. Dees, Country Boy Trailers, to FCC, CG Docket No. 03-123 (June 1, 2006) (“Country Boy Trailers June 1 *ex parte*”).

calls while still meeting the FCC's speed-of-answer requirements. Such overstaffing decreases providers' efficiency and increases their costs.

The fraudulent misuse of IP Relay will, if unchecked, effectively lessen the availability of the service by thwarting both its use and usefulness for legitimate purposes. This cannot be squared with the ADA, which requires the Commission to "ensure" that all forms of TRS, including IP Relay, are "available to the extent possible," to all deaf, hard-of-hearing, and speech-disabled individuals.⁹ The Commission therefore must act to curb the fraudulent use of IP Relay now, before it is too late.

B. The FCC Should Require Providers to Take Appropriate Actions to Reduce IP Relay Fraud

To be effective, any FCC action in this proceeding must be predicated on the fact that perpetrators of fraud are agile and determined, and will attempt to outwit any solution. The FCC's goal, therefore, should be to enable solutions that, on the one hand, are sufficiently flexible to respond to the changing tactics of perpetrators, but, on the other hand, narrowly target fraud without impairing the ability of legitimate callers to place and receive IP Relay calls.¹⁰

The best way to achieve these ends would be to require providers to implement a dual solution: (i) block international calls; and (ii) flag calls that meet certain indicia of fraud, subject to safeguards designed to prevent legitimate calls from being refused or otherwise impaired. Each of these measures is described below.

As noted, many fraudulent IP Relay calls are placed by persons located outside of the United States. Blocking a significant percentage of these calls is feasible, both legally

⁹ 47 U.S.C. § 225(b)(1).

¹⁰ *See Further Notice* ¶ 15.

and technically. Providers are not required to carry international IP Relay communications, and in fact are not even reimbursed for such calls.¹¹ It is therefore lawful for providers to block international IP Relay calls. Doing so also is technically feasible. In fact, Sorenson currently blocks international calls by resolving IP addresses using geo-location services.¹² This helps prevent international calls from getting into the queue of IP relay calls to be handled by a Sorenson CA. As a result, a significant portion of fraudulent calls never reach a Sorenson CA. The FCC should include the blocking of international calls as part of any solution it mandates.

Blocking should be only one part of any ongoing solution, however. Not all fraudulent IP Relay calls are international, and even where the call is international, resourceful perpetrators can devise ways to circumvent blocking – *e.g.*, by simulating or “spoofing” a domestic call. The Commission therefore should supplement blocking with the additional measures described below.

As the Commission recognized in the *Further Notice*, “there are many readily identifiable indicia of [fraudulent] IP Relay calls.”¹³ Using these indicia, a CA can

¹¹ See *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123, Declaratory Ruling on Reconsideration, 21 FCC Rcd 5962, ¶ 9 n.23 (rel. May 25, 2006) (DA 06-1100).

¹² Like area codes for traditional North American Numbering Plan (“NANP”) numbers, IP addresses usually indicate the general geographic region of the user of that address. There are services available that allow providers to associate the IP address of each caller with the geographic region indicated by that address. Providers can then block all calls from any addresses associated with a non-U.S. location. Although this method is effective at identifying some international calls, it cannot capture all calls placed from locations outside the United States. For example, perpetrators located outside the United States can obtain an IP address associated with a geographic location within the United States. For this reason, the Commission should supplement blocking by adopting the call-flagging process described below.

¹³ *Further Notice* ¶ 13.

usually identify calls that are fraudulent. The Commission should take advantage of this ability by working with the Consumer Advisory Committee (“CAC”) and providers to develop a non-public list of criteria that can be used to identify fraudulent calls without harming the interests of legitimate users.¹⁴ This list easily could be updated to reflect the changing tactics used by perpetrators of fraud. It is critical, however, that any such list remain confidential: Neither the criteria recommended by the CAC or providers, nor the list approved by the FCC, should be disclosed or made available to the public. Doing so would only give the perpetrators of fraud a roadmap of how to circumvent the criteria. The Commission therefore should issue a protective order under which access to the recommended and approved list would be limited to certified providers of IP Relay and their attorneys.

Once an FCC-approved list of criteria is adopted, providers would be able to implement the following simple process to root out fraudulent IP Relay calls:

- Relying on the FCC-approved list, CAs would identify a potentially fraudulent call.
- The CA’s supervisor would then assess the call and independently verify the CA’s judgment.
- If the CA and the supervisor agreed that the call was potentially fraudulent, the CA would read aloud to the hearing party and type to the deaf party a brief, FCC-approved message that would allow either party the option of terminating the call. If the parties chose to remain on the line, the call would continue as before. The CA would never terminate a call on his or her own discretion.

The foregoing process would have a number of advantages: It would maximize the likelihood that only fraudulent calls are flagged; it would be easy to implement; it

¹⁴ Providers have an incentive not to recommend overly broad criteria. Providers want to handle (and be reimbursed for) as many calls as possible, provided they are legitimate. Providers do not want to develop a reputation among the deaf community for interrupting legitimate calls.

would afford providers flexibility in responding to the ever-changing tactics of perpetrators; and it would protect the interests of legitimate users.¹⁵ Multiple safeguards are built into this process to minimize the CA's discretion and the likelihood of "false positives." Even if a call were flagged by both the CA and his or her manager, the parties would be simply prompted to decide whether to end the call – something either party already can do at any time.

The Commission could further protect the interests of legitimate users by adopting rules designed to guide the exercise of discretion by the CA and his or her supervisor.¹⁶ For example, the following guidance would be appropriate: (1) Callers may be prompted by the CA only if both the CA and his or her supervisor agree that the call meets one or more of the criteria established to identify fraudulent calls; (2) A prompting shall consist solely of a standard script that informs both parties of the fact that a call has been identified as potentially fraudulent, and asks the parties if they wish to remain on the line; (3) A call flagged as potentially fraudulent shall not be discontinued unless one or both of the parties to the call chooses to end the call (a CA shall not unilaterally discontinue a call); and (4) No provider or CA shall retain records of the content of potentially fraudulent calls, including calls that have been terminated.

In addition to any such guidelines, the Commission should clarify that providers should be compensated for any conversation minutes they handled before a fraudulent

¹⁵ The recommended approach also would allow providers to continue to use technology to block illegitimate uses of IP Relay. Technology has its limits, however – particularly since the perpetrators of fraud work diligently to overcome any impediments to the success of their fraudulent schemes. That is why it is critically important to supplement any technological barriers to fraud with a more flexible response, based on non-public, FCC-approved criteria that can be readily adjusted to match the changing tactics of perpetrators.

¹⁶ See *Further Notice* ¶ 12.

call was terminated. By blocking international calls, providers likely will have screened a large portion of fraudulent calls. Providers will receive no compensation for such blocked calls. There should be a presumption that all non-blocked calls are legitimate – and therefore compensable – up until such point as the call is voluntarily terminated, pursuant to the procedure outlined above.

C. Other Approaches Would Not Be Effective

Other approaches to combating the fraudulent use of IP Relay would not be nearly as effective as the dual solution, described above, of requiring providers to block international calls and flag potentially fraudulent calls. The *Further Notice* seeks comment on the efficacy of requiring end-user “registration as a means of curbing illegitimate IP Relay calls.”¹⁷ Although Sorenson supports voluntary registration as a means of enhancing service,¹⁸ a voluntary registration scheme would fail to curb IP Relay fraud since the perpetrators of fraud could simply opt not to register. Mandatory registration also could be easily circumvented by the perpetrators of fraud, and would be cumbersome and intrusive as well. For example, a person bent on perpetrating fraud could register under a fictitious name and then use that false registration to place a fraudulent order via IP Relay. If the provider subsequently blocked any calls placed under the false registration, the perpetrator could simply re-register by providing a different set of false information (*e.g.*, a new name). Because the provider has no way of verifying whether the identifying information submitted by a registrant is accurate, the

¹⁷ *Id.* ¶ 14.

¹⁸ *See, e.g.*, Comments of Sorenson Communications, Inc., CG Docket No. 03-123, at 15-16 (Feb. 22, 2006) (“Sorenson 911 Comments”) (favoring voluntary registration, but opposing mandatory registration, as a means of facilitating access to emergency services).

provider is powerless to prevent perpetrators from using serial registration as a means to commit fraud under various aliases.¹⁹

Any mandatory registration scheme also would be intrusive, requiring users to disclose sensitive personal information. Many legitimate users might seek to avoid this requirement by providing false information²⁰ or ceasing to use IP Relay altogether – a result that would be contrary to the ADA’s goal of ensuring greater availability of relay services.

Other potential solutions would also be wholly or largely ineffective. For instance, although providers should be able to use technology to help prevent fraudulent calls from getting through to a CA, blocking calls from an IP address that was previously used to commit fraud would provide only limited benefits: Because most IP addresses are dynamic and can change from call to call, there is often little likelihood that the same address would be used more than once to place a fraudulent call via IP Relay.²¹

D. Sorenson’s Proposed Solution Would Be Legally Sound

The dual solution of blocking international calls and flagging other potentially fraudulent calls would be legally sound. As noted, IP Relay providers are not required to

¹⁹ As the *Further Notice* explains, because IP Relay calls are transmitted via the Internet, they do not inherently transmit any personally identifying information about the caller. By contrast, because TTY calls are made over the PSTN, “the call to the relay center includes identifying information, such as the calling party’s number.” Such identifying information deters the misuse of TTY “because the relay provider knows where the inbound call is coming from.” *Further Notice* ¶ 6 n.19.

²⁰ In Sorenson’s experience, some users have avoided registration requests by providing fictitious or inaccurate information. See Sorenson 911 Comments at 15 n.29.

²¹ Dynamic IP addresses remain in place for varying periods of time, and can change after as little as 15 minutes.

handle international calls.²² Therefore, blocking international calls clearly is legally permissible.

Flagging also would be consistent with all provisions of the ADA and the Commission's implementing rules. For instance, Sorenson's proposed solution would not authorize the CA to alter any of the words spoken or typed in the relayed conversation.²³ Furthermore, under Sorenson's proposed solution, providers would continue to accept all domestic calls and would never unilaterally terminate any call.²⁴ Providers also would not disclose the content of a call to any third party or make or keep records of such content.²⁵ Instead, providers would, at most, keep records of the fact that a particular call had been flagged as potentially fraudulent under the criteria established by the Commission.²⁶

²² See *supra* note 11.

²³ See 47 U.S.C. § 225(d)(1)(G) (prohibiting CAs from "intentionally altering a relayed conversation"); see also 47 C.F.R. § 64.604(a)(2)(ii) (same). As noted, Sorenson's solution would require a CA to read/type a short script for calls flagged as potentially fraudulent. This interjection would not "alter" the relayed conversation. CAs frequently interject words into IP Relay conversations. For instance, a CA may ask the hearing party to repeat a sentence or to speak more slowly. The interjection of a brief standard script designed to alert parties to the possibility of fraud would be consistent with these practices.

²⁴ See 47 U.S.C. § 225(d)(1)(E) (prohibiting providers from "refusing calls or limiting the length of calls that use telecommunications relay services"); see also 47 C.F.R. § 64.604(a)(3)(i) (same).

²⁵ See 47 U.S.C. § 225(d)(1)(F) (prohibiting relay operators from "disclosing the content of any relayed conversation and from keeping records of the content of any such conversation beyond the duration of the call"); see also 47 C.F.R. § 64.604(a)(2)(i) (same). Sorenson has taken a number of steps to ensure the privacy and security of Relay calls. See Sorenson 911 Comments at 15-16.

²⁶ The *Further Notice* seeks comment on whether section 705 of the Act would restrict the Commission's authority to take actions to curb the fraudulent use of IP Relay. *Further Notice* ¶ 16 & n.40; 47 U.S.C. § 605(a). Although it is not clear that section 705 even applies to TRS CAs or their supervisors, Sorenson is confident that, if section 705

To the extent necessary, the FCC should clarify that the solution proposed herein is consistent with its rules and policies.²⁷ As an alternative (or in addition) to any such clarifications, the FCC could find that calls that meet certain criteria (such as those set forth in the non-public list approved by the FCC) are presumptively not placed by a deaf, hard-of-hearing, or speech-disabled person, and therefore those calls do not meet the definition of TRS.²⁸ Such non-TRS calls are not entitled to the protections of section 225 or the FCC's rules implementing that section. Finally, if necessary, the Commission should waive or modify any FCC rule, or forbear from enforcing any provision of the Act, that potentially would not be consistent with the solution proposed herein.

E. The FCC Should Authorize CAs and Interpreters to Terminate Any TRS Call that Is Obviously Illegitimate

In certain scenarios, a CA or interpreter can readily discern that a call placed to a Relay provider does not involve a deaf, hard-of-hearing, or speech-disabled person, and hence is not a legitimate TRS call under the ADA.²⁹ The Commission should authorize CAs or interpreters to terminate those calls.

were deemed applicable, the solution proposed herein could be implemented in a way that is consistent with that section.

²⁷ For example, the FCC has previously described the CA as a “transparent” entity who “may not interfere with the [relayed] conversation,” and has stated that CAs should not “have a law enforcement role by monitoring the conversations they are relaying.” *Further Notice* ¶ 9 (citations omitted). If necessary, the Commission should clarify that these policies are consistent with requiring CAs to read a standard script once a call has been flagged as potentially fraudulent, or that such a practice is a narrow exception to those FCC policies. *See Further Notice* ¶ 11 n.37 (noting that in other contexts, the FCC has permitted the CA to step out of the role of strictly being a transparent conduit that relays the call).

²⁸ *See* 47 U.S.C. § 225(a)(3).

²⁹ *Id.*

For example, some prisoners have begun to use speech-to-speech services to make free long-distance calls. The CA should be able to terminate such calls if, for example, he or she hears both parties speaking clearly and not waiting for the CA to interpret either end of the call. Likewise, some individuals place VRS calls as a substitute for in-person interpreting or Video Relay Interpreting.³⁰ A VRS interpreter should be able to terminate such calls if, for example, he sees both the calling and called party sitting side-by-side in the same room.

There is no need for the Commission to adopt rules to guide the discretion of the CA or interpreter to terminate calls that are patently illegitimate.³¹ The CA or interpreter is in the best position to identify such calls, and the Commission should trust the common sense of the CA or interpreter to take appropriate action, as it has in other contexts.³² The provider should not be required to maintain records of any terminated call (other than to note that the call was terminated as illegitimate), and should be compensated for the conversation time prior to any such termination.³³ As explained above with respect to IP Relay calls, there should be a presumption that all calls are legitimate – and therefore compensable – up until such point as the CA/interpreter discerns that a call is obviously illegitimate and terminates the call.

³⁰ See *Further Notice* ¶ 10.

³¹ See *id.* ¶ 18.

³² See *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123, Order, FCC 06-81, ¶ 9 (rel. June 16, 2006) (affording VRS interpreter discretion to be replaced by another interpreter when “the party using sign language, the CA, or both, find that they are unable to communicate effectively,” without violating the 10-minute in-call replacement rule).

³³ See *Further Notice* ¶ 20.

III. CONCLUSION

To curb the fraudulent use of IP Relay, the Commission should require providers to block international calls and flag other potentially fraudulent calls, pursuant to the process described above. The Commission also should authorize CAs and interpreters to terminate any call whenever it is readily apparent that such calls are not legitimate Relay calls.

Respectfully submitted,

/s/ Gil M. Strobel

Gil M. Strobel
Richard D. Mallen
Lawler, Metzger, Milkman & Keeney, LLC
2001 K Street NW, Suite 802
Washington, DC 20006
(202) 777-7700
gstrobel@lmmk.com

Michael D. Maddix
Product Manager
4393 South Riverboat Road
Suite 300
Salt Lake City, Utah 84123

July 3, 2006