

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 )

To: Secretary, FCC  
For: The Commission

**COMMENTS OF HAMILTON RELAY, INC.**

Hamilton Relay, Inc. (“Hamilton”), by its counsel, hereby submits comments in response to the Commission’s *Further Notice of Proposed Rulemaking* regarding the misuse of Internet Protocol relay services (“Internet Relay”) and Video Relay Services (“VRS”).<sup>1</sup> Attempts to misuse Internet Relay are among the most difficult calls for providers to handle, because they require time-consuming efforts to track down and block calls from known fraudulent IP addresses. More importantly, they are an emotional drain on Communications Assistants (“CAs”) and ultimately undermine the relay service. Failure to address these calls places the relay system at risk by undermining the credibility of legitimate relay users, and may even jeopardize relay funding. Accordingly, Hamilton is encouraged by the Commission’s

---

<sup>1</sup> *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, CG Docket No. 03-123, FCC 06-58 (rel. May 8, 2006) (“*FNPRM*”).

efforts to find a workable, legal solution to the vexing problem of fraud and misuse of Internet-based relay services.

As the Commission has noted, due to the transparent nature of the CA's role in a TRS call, the CA may not interfere with the conversation.<sup>2</sup> The prohibition of CA interference is statutory — CAs are prohibited 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” and from “intentionally altering a relayed conversation.”<sup>3</sup> Further, Section 705 of the Communications Act of 1934, as amended (“Communications Act”) prohibits persons assisting in receiving or transmitting interstate or foreign communications to divulge the contents of the communication unless authorized by law.<sup>4</sup> The disclosure of relay call content also would appear to violate the Electronic Communications Privacy Act.<sup>5</sup> For these reasons, Hamilton opposes waiving or modifying the TRS rules to allow Internet Relay and VRS providers and their CAs to terminate calls they presume are not legitimate calls.<sup>6</sup> In addition, there are seemingly endless situations in which a CA

---

<sup>2</sup> *FCC Reminds Public of Requirements Regarding Internet Relay Service and Issues Alert*, Public Notice, DA 04-1738, at 1-2 (rel. June 18, 2004) (“*Fraud Public Notice*”).

<sup>3</sup> *Id.* § 225(d)(1)(F).

<sup>4</sup> 47 U.S.C. § 605.

<sup>5</sup> 18 U.S.C. § 2511.

<sup>6</sup> *FNPRM*, ¶¶ 11-13. Requiring or permitting a CA to intervene during a fraudulent call in process is different than allowing speech-to-speech CAs to briefly step out of their role of being a transparent conduit. The former would require a conscious decision by the CA to terminate a potentially legitimate call, whereas the latter simply permits an STS CA to retain information from a previous call to help (continued...)

could decide it is appropriate to terminate a call: credit card fraud, sale of alcohol to minors, conspiracy to commit a felony, and numerous other activities that the CA may find to be illegal, immoral, or distasteful. Allowing a CA to exercise individual judgment about call content and to determine whether or not a call should be terminated inevitably would be contrary to statutory prohibitions, and is likely to violate the very rights the ADA was designed to protect. Censoring the conversations of relay users is not acceptable.

While there are clear legal impediments to the interruption of calls by CAs, Hamilton believes that there are legitimate methods available to further discourage misuse of Internet Relay and VRS. Hamilton already has taken steps to deter fraud in a manner that it believes is consistent with the Communications Act, the ADA, and FCC rules. For example, Hamilton routinely blocks international IP addresses from accessing its Internet relay service.

The types of calls that the Commission is seeking comment on are nothing new — these calls likely have occurred since the inception of TRS more than fifteen years ago, and in fact occur occasionally outside of the TRS world. It is Hamilton's belief that the reason these calls have escalated so dramatically lies squarely with the addition of IP-enabled relay, and the general perception that the Internet provides a veil of anonymity, and thus a lack of accountability. This perceived anonymity is, for the most part, nonexistent in the traditional TRS world because

---

facilitate future calls. The other situations cited by the Commission are merely proposals that may or may not be adopted. *See id.* n.37.

relay is accessed by the public switched telephone network (“PSTN”). With the increasingly rare exception of payphones, each traditional relay call originates from a telephone customer that has subscribed for local service with a telecommunications carrier. One requirement for such a subscription is to provide a name and billing address. Although this subscriber information is kept confidential in accordance with state and federal Customer Proprietary Network Information guidelines, it is made available to law enforcement agencies when a court of competent jurisdiction directs the carrier to do so. The recognition of this accountability has been a far more effective deterrent to abuse of the system than CA intervention could ever come close to providing.

### Registration

Hamilton believes that finding a functionally equivalent way to restore the level of accountability that has historically existed with traditional relay is the best way to deter misuse of the relay system. One of the most effective and least invasive means would be a registration system for Internet Relay and VRS that is consistent with the customer information of subscribers to carriers using the PSTN.<sup>7</sup> To be effective, the registration system would need to: a) be mandatory for all Internet Relay and VRS users; b) be mandatory for providers to implement and interoperable among providers; and c) protect the privacy of relay users.

---

<sup>7</sup> See *FNPRM* ¶ 14 (proposing a registration system).

Under this system, all users would be required to register the User ID that they would use to contact their relay provider of choice. In order to safeguard the privacy of users, Hamilton suggests that a competitively neutral third party be used for registration purposes. To register, the user would need to provide the neutral third party with uniquely identifiable information routinely used for online registrations, such as name, address and telephone number (but not a Social Security Number or other sensitive information). The neutral third party could use one of the commercially available means for verifying the user information. Once validated, the user's information would be kept as proprietary information by the neutral third party, and released only to authorized law enforcement with a valid subpoena. The User ID alone would be automatically available to all providers, in much the same fashion as an ANI is currently provided to traditional relay providers upon call arrival. In other words, no customer proprietary network information would be available to relay providers — only a User ID would be available.

Under this scenario, if a user registers with a neutral third party as “TRS User 1”, that User ID would be recognized and accepted by all relay providers without any noticeable delay in call set-up, regardless of which provider TRS User 1 chooses to use to place that call. Registration information would have been validated already by the neutral third party at the time of registration; thus, the relay user should experience no delays. If the user has not yet registered, he or she would be directed to register first with the neutral third party and then, once

registered, he or she could return to the relay provider of choice. Costs associated with establishing and maintaining the registration system should be reimbursable from the interstate TRS Fund.

Although the initial registration requirement may be viewed as an inconvenience to some relay users, Hamilton believes that the benefits to combating misuse outweigh any minor inconveniences. All subscribers to the PSTN register by virtue of their subscription to local service, and most online users must register in some form before using an online service; Internet Relay and VRS should be no different. In addition, a registration system would be consistent with the Communications Act because it would not require the CA to intervene in any way with a relay call.

Finally, while Hamilton supports the use of a registration system as a means of deterring fraud, Hamilton does not support the use of a registration system as a proxy for determining separation of costs, for the reasons set forth in previously filed comments.

#### VRI Calls

The Commission is also seeking comment on whether VRS is being misused as a substitute for in-person interpreters or as a Video Remote Interpreting (“VRI”) service. Hamilton believes that it is far easier to prevent this type of abuse than Internet Relay fraud, because with VRS there is visual confirmation of misuse. The degree of anonymity available with Internet Relay is simply not present with VRS. Hamilton has instructed its CAs that if two or more persons are present in a room

and request VRS services, the CA must call a supervisor to confirm and, if confirmed by the supervisor, the CA informs the parties that the service can only be used for VRS calls, not VRI or in-person interpreting. The users are then prompted to make a legitimate VRS call or have the call terminated. Hamilton encourages the Commission to clarify that VRS providers may refuse to handle a call if a CA, when setting up the call (i.e., prior to commencing the call), can determine visually that the call is not a VRS call. The refusal of a CA to handle such a call is consistent with Section 225(d)(1)(E) of the Communications Act because the call is not a legitimate relay call.<sup>8</sup>

#### Conclusion

Hamilton continues to oppose any FCC rule requiring the CA to step out of his/her role as an invisible conduit of relay calls, because such a requirement is fundamentally at odds with the statutory mandates of the relay service. However, Hamilton supports a registration system if it is centralized, mandatory, and protects the privacy of users. With respect to VRS misuse, Hamilton requests that the Commission clarify that CAs may refuse to set up a VRS call if the CA can visually confirm that the service is intended to be used for in-person interpreting or VRI.

Respectfully submitted,

---

<sup>8</sup> In contrast, an Internet Relay CA cannot determine whether a text-based call is fraudulent or not until the call has commenced, at which point the CA is prohibited from intervening. Additionally, an Internet Relay call may legitimately be made even if the call is for a dubious purpose.

HAMILTON RELAY, INC.

/s/ David A. O'Connor

David A. O'Connor

Holland & Knight LLP

2099 Pennsylvania Ave., NW

Suite 100

Washington, DC 20006

Tel: 202-828-1889

Fax: 202-955-5564

E-mail: david.oconnor@hklaw.com

*Counsel for Hamilton Relay, Inc.*

July 6, 2006

*Submitted via ECFS*

# 3887265\_v5