

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

In the Matter of)	
)	
Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities)	CG Docket No. 12-38
)	
Misuse of Internet Protocol (IP) Relay Service and Video Relay Service)	
<hr/>)	

COMMENTS OF SPRINT NEXTEL CORPORATION

Sprint Nextel Corporation ("Sprint"), on behalf of the Telecommunications Relay Services ("TRS") operations of its subsidiary, Sprint Communications Company L.P., hereby respectfully submits its comments on the issues raised in the *Public Notice* (DA 12-208) issued February 13, 2012 by the Consumer and Government Affairs Bureau (Bureau) of the Federal Communications Commission ("FCC" or "Commission") in the above-captioned proceeding "pertaining to misuse of Internet Protocol (IP) Relay Service" ("IP Relay"). *Public Notice* at 1.

INTRODUCTION

The Bureau notes that in 2006, the FCC issued a *Further Notice of Proposed Rulemaking* in CG Docket No. 03-123, 21 FCC Rcd 5478 (2006 FNPRM) seeking comments on the problem of "individuals who do not have a hearing or speech disability ... misus[ing] IP Relay by, for example, calling merchants to place orders using fake, stolen, or otherwise invalid credit cards," *Public Notice* at 1, and since that time "has undertaken a number of measures to combat [such] misuse of the IP Relay Program." *Id.* at 2. According to Bureau, the most significant FCC

initiative in this regard was the adoption of the requirement that every person with a hearing or speech disability, who wishes to use an IP-enabled Relay service, including IP Relay service, to make and receive calls, register with his/her IP Relay provider of choice (default provider) and obtain a ten-digit telephone number linked to the North American Numbering Plan from such provider.¹ The Bureau goes on to explain that in a subsequent decision the FCC imposed additional requirements on providers of Internet-enabled Relay services which the FCC expected would help “curtail illegitimate calls made through [IP Relay] service.” *Id.* at 2. Providers of IP-enabled Relay services were required (1) “to ‘implement a reasonable means of verifying registration and eligibility information,’ including the consumer’s name and mailing address, before issuing the consumer a ten-digit telephone number”; (2) to conduct a “consumer education and outreach [program] to inform [IP Relay] users of the importance of providing accurate registration information”; and (3) to include in their “verification procedures ... a self-certification component requiring consumers to verify that they have medically recognized hearing or speech disability necessitating their use of TRS.”² The Bureau, however, points out that “[d]espite the Commission’s persistent efforts to combat the fraudulent use of IP Relay,” *Public Notice* at 5, the misuse appears to have continued. Thus, the Bureau has asked for the views of the various interested parties on ways to enhance these efforts. Sprint’s views in this regard follow.

¹ *Public Notice* at 2 citing *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; E911 Requirements for IP-Enabled Service Providers*, 23 FCC Rcd 11591 (2008).

² *Public Notice* at 2-3 citing *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; E911 Requirements for IP-Enabled Service Providers*, 24 FCC Rcd 791, 809-810 (2008).

DISCUSSION

Some IP Relay providers may have decided to rely entirely the FCC's 10-digit numbering regulatory regime to combat IP Relay fraud because they share the FCC's belief that such program would be highly effective in controlling and minimizing such fraud. Sprint, however, has long doubted that this regime alone could address the FCC's concerns in this regard and although Sprint, like all IP Relay providers, has limited resources to devote IP fraud detection and prevention, it has implemented a number of anti-fraud measures.

Sprint, of course, fully complies with the requirements imposed by the FCC's 10-digit numbering regime. For example, Sprint has retained the services of one of the leading suppliers of both online/real-time identity verification solutions to ensure that the name and address of the registrant provided during the registration process are valid. Such supplier compares the information received from Sprint with the information in its databases which consists of public and commercially available information such as voter registration, motor vehicle information, property records and social security records. It then transmits the results of this comparison back to Sprint. If the results confirm that the information the user has provided is accurate the user is able to complete the registration process by obtaining a ten-digit number. If not, the potential entrant cannot complete the registration process.³ Moreover, through its IP Relay products,

³ Sprint also sends an email to the email address provided by the registrant informing the registrant that the registration process has been successfully completed and providing the registrant with his/her ten-digit number. Although it may be costly to do so, Sprint is currently considering the possibility of developing and implementing a method to enable it to verify the email address during the registration process; if the email address cannot be verified, Sprint would terminate the registration process and not assign a ten-digit number to the registrant.

Sprint is able to check the IP address to ensure that such registrant is using a device located in the United States.

As stated, however, no one method can be relied upon to effectively control the fraud problem. This is so because through such fraudulent activities, criminals located in such places as Nigeria, Ghana and Russia can reap substantial sums of money with little, if any, risk of arrest and prosecution in their home countries. Thus, these individuals have the incentive and the means to develop ways to evade any one solution implemented by an IP Relay provider.⁴ For this reason, Sprint has employed and continues to employ a number of methods designed to deal with the IP-Relay fraud problem. Sprint's methods are based on and informed by its long-standing efforts to minimize, if not eliminate, the use of its IP Relay service by individuals seeking to defraud merchants by making purchases over the telephone using stolen, fake, or otherwise invalid credit cards and to make harassing calls.”⁵

As Sprint explained in its comments in response to the *2006 FNPRM*, shortly after discovering the problem, Sprint constructed a database consisting of IP addresses that Sprint determined were being used to make IP Relay calls from international locations. Sprint then

⁴ At various meetings with FCC staff to discuss a 10-digit numbering regime prior to its adoption, Sprint's representatives would often make the point that although the requirement that users of IP-enabled Relay services obtain a 10-digit number was in the public interest, especially since such requirement would likely enhance the ability of such users to obtain timely access to emergency services, it was somewhat unrealistic to expect that a 10-digit numbering regime would have a significant effect of mitigating the IP-Relay fraud problem and should not be relied upon as the sole means for minimizing the problem.

⁵ *2006 FNPRM* at ¶6. In 2004, Sprint learned that individuals in foreign countries, such as Nigeria, were using Internet Relay to fraudulently obtain goods from businesses in the US. It informed the FCC of the problem – apparently the first, and perhaps only, IP Relay provider to do so – see *Ex Parte* Letter dated February 18, 2004, from Michael B. Fingerhut, Attorney for Sprint to Marlene Dortch, Secretary to the FCC in CG Docket No. 03-122 and CC Docket No. 98-67 – and shortly thereafter began taking steps to minimize the fraud.

blocked (and continues to block) calls to its Relay centers from the IP addresses in its database.

Although costly to develop and maintain, this method was, and continues to be, effective in controlling the volume of IP Relay calls from international locations.⁶

Unfortunately, even Sprint's IP address blocking mechanism, which has been an effective method in combating fraudulent calls, cannot be relied upon to totally prevent a fraudulent IP Relay call from an international location to a merchant located in the US. Indeed, Sprint believes that many of these fraudulent operations are now obtaining IP address from American companies providing hosting services in foreign countries and the call would appear to have originated from a domestic rather than a foreign location. Thus, Sprint continues to utilize its "call intervention program" in an effort to minimize the use of IP Relay to obtain goods from merchants illegally.⁷

Sprint notes that this program continues to prevent many thousands of merchants from falling victim to these scams, much to their appreciation. Indeed, upon being placed on hold so that the Sprint communications assistant/supervisor can advise the merchant that the IP Relay caller may be engaged in what appears to be fraudulent activity because of certain traits common

⁶ Sprint recognizes that it is database cannot possible include all IP addresses that fraudulent users may use to access the IP Relay services of providers. Thus, the FCC may wish to consider establishing an industry-wide database that providers can access during the registration process to help determine whether the person seeking to register with the IP Relay provider in order to receive a ten-digit number and thereby make IP Relay calls has accessed the provider's on-line registration page using a US-based device.

⁷ In its FNRPM Comments (at 4-6) Sprint explained the program and why the program did not implicate the requirements of Section 225 of the Act and the FCC's regulations issued thereunder, and need not repeat such explanation here. Although the FCC in the *FNPRM* (at ¶11) expressed skepticism about those intervention programs (such programs "may [be] creat[ing] tension with the functional equivalency principle"), but it now appears to accept Sprint's position that most if not of all these fraudulent calls are being made by those without a hearing or speech disability and thus such calls are not relay calls within the meaning of Section 225. *See Public Notice* at 1.

to such calls, the IP Relay caller often will terminate the call on his/her own initiative since such caller knows that the merchant from whom he/she is trying to illegally obtain goods will usually choose to authorize Sprint to discontinue the call.

Sprint also continues to implement methods to enhance its ability to identify whether its service is being misused and thus be better position to quickly take steps to minimize such fraud. For example, a daily report of the number of IP Relay calls from each IP address is produced so as to enable Sprint's analysts to determine whether the IP Relay minutes being generated from that address have increased above expected levels. If so, and because such elevated levels could be evidence of fraudulent calling, Sprint will, after further investigation, block calls coming from such address. Similarly, Sprint will also block calls from any IP address or IM screen name that is generating a high volume of calls usually within a specified period of time. Finally Sprint continues to explore additional approaches that could be used to minimize, if not eliminate, the misuse of its IP Relay service.

Sprint mentions its IP Relay fraud detection and remediation programs not only because such methods have been effective in minimizing the use of its IP Relay service for fraudulent purposes – Sprint's volumes have been relatively stable and it does not experience with any frequency the types of traffic spikes that may be indicative of fraudulent calling – but also because Sprint believes it to be important to emphasize that it has implemented such programs and is looking to improve upon them on its own initiative without being required to do so by FCC mandate. In fact, the prescription of a detailed regulatory framework by the FCC could be counterproductive. Certainly, a detailed regulatory structure would limit an IP Relay provider's flexibility to quickly adapt current procedures or implement new ones as circumstances warrant. It may also provide bad actors a roadmap for ways to circumvent those fraud prevention

procedures. The Commission should be careful not to specify the manner in which limited resources are used in fraud prevention. Greater flexibility, rather than specific prescriptions are more likely to be successful.

In short, no one method can reasonably be relied upon to eliminate the fraudulent use of IP Relay. By opposing the creation of a new regulatory regime, Sprint is not suggesting that IP Relay providers ignore their responsibility to attempt to minimize the misuse of their IP Relay service. Rather such providers should be expected to take reasonable steps to detect and control such fraud. The FCC should continue to monitor providers' efforts in this regard and take appropriate action if a provider fails to take such steps.

Respectfully submitted,

SPRINT NEXTEL CORPORATION

A handwritten signature in black ink, appearing to read "Michael B. Fingerhut", is written over a horizontal line.

Michael B. Fingerhut
Charles W. McKee
900 7th Street NW
Washington, D.C. 20001
(703) 592-5112

Its Attorneys