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

In the Matter of	)	
	)	
Consumer & Governmental Affairs Bureau Seeks To Refresh The Record Regarding 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

To the Commission

COMMENTS OF AEQUUS TECHNOLOGIES CORPORATION

Aequus Technologies Corporation ("Aequus") hereby submits its response to the Consumer and Governmental Affairs Bureau's *Public Notice* seeking comment to refresh the record regarding misuse of Internet Protocol Relay Service ("IP Relay") Service.[1]

Aequus welcomes the opportunity to comment on concerted efforts by the Federal Communications Commission's ("Commission") to refresh the record toward elimination of waste, fraud and abuse perpetuated by those who misuse IP Relay services and by IP Relay service providers who knowingly allow such to occur in order to receive reimbursement from the iTRS Fund.

Aequus wishes to commend the Commission for its adoption of rules in recent years to protect the integrity of the IP Relay program so that this service remains sustainable and ensures functionally equivalent telecommunications for deaf and hard of hearing users.

Aequus recognizes the fact that the Commission intends to undertake additional steps through this proceeding to combat IP Relay waste, fraud and abuse prior to taking decisive action on currently pending applications for IP Relay certification submitted by Aequus and other parties.

---

[1] *Consumer & Governmental Affairs Bureau Seeks To Refresh the Record Regarding Misuse of Internet Protocol Relay Service,* Public Notice, DA 12-208 (rel. Feb. 13, 2012) *("Notice");* see also *Comment Cycle Established for Comments to Refresh the Record Regarding Misuse of Internet Protocol Relay Service,* Public Notice, DA 12-308 (rel. Feb. 28, 2012)

I. Verification Methods

Aequus supports the use of a dual-track registration process to authenticate the identity and eligibility of individuals seeking to obtain a ten-digit number for IP Relay purposes. Such a process would entail provision of relevant contact specifics, including physical address, necessary to populate the Registered Location database. This can be done through several methods, via web-based registration, customer service contact or directly with the Communications Agent ("CA") – the applicant would either establish or receive a username and password for his or her web-based customer account. Once initial information is collected, the provider's registration system would carry out two automated tasks: 1) send the applicant an email, requiring a clickable web link to verify the email address as being legitimate (if the email is not verified by applicant response within 24 hours, the account is deactivated), and 2) send a postcard to the applicant's physical address via the U.S. Postal Service, containing a second web link and passcode (one-time personal identification number) whereupon the applicant would be required to log onto his or her web-based account with the same username and password used at the time of account set up. Physical addresses are also verified through third-party vendor arrangements, e.g., Intelius (www.intelius.com), along with additional tools for this purpose. If the applicant's physical address is not verified within five business days, the account is deactivated. Once these steps are completed, the applicant is verified for ten-digit number issuance. Applicant records are retained within the local database, the new TDN is provisioned along with the applicant's routing information to the iTRS database, the applicant is notified of his or her new TDN and advised on collection of customer proprietary network information in accordance with Commission rules as well as the importance of and how to make timely updates to their registered location for emergency purposes.

II. Effectiveness of Verification Measures

Aequus believes that the dual track verification process delineated above works very well in combating IP Relay fraud and misuse, with the appropriate infrastructure in place and when properly conducted by experienced personnel. Trained personnel can uncover physical address redundancies at the

time of registration, aided by database filters designed to take note of such, taking steps to ensure that additional registration requests originating from the same address are genuine.

Aequus does not recommend in-person or on-camera ID checks during registration, as such would be cumbersome, absent, or inapplicable within a text-rich communications environment. Additionally, IP Relay outreach efforts are targeted to hard of hearing individuals who are increasingly making use of and relying upon text relay as a solution for their telecommunications needs.

III. Unlawful Registration Practices

Aequus has detected calls of fraudulent nature by users registered with other providers, and has accordingly notified the Commission and to the U.S. Department of Justice of such occurrences. These typically involve dial-around calls that draw immediate suspicion and can be caught once their call is made to a hearing party. Aequus is concerned that in the absence of rigorous Commission rules for IP Relay registration, there is greater potential for fraudulent users to target a specific provider they perceive as having the least stringent registration practices. All calls involving questionable registration information and/or known fraudulent call content patterns should be immediately disconnected and internal flags activated to block future call attempts. This underscores the importance of the Commission instituting uniform and rigorous provider verification processes for users seeking ten-digit numbers for IP Relay purposes.

IV. Preventive Measures Against Unlawful Registration

Aequus believes that IP Relay fraud is a two-pronged problem, and both must be vigorously addressed to eliminate waste and abuse. More rigorous registration processes can effectively combat the first type of fraud involving misuse perpetrated by those who mask their true identities and who seek to commit fraud against those whom they call via relay. The second type of fraud – equally as serious – is a byproduct of these calls, whereas providers opt to process them so they can collect monies from the iTRS Fund. Establishment of a centralized database to combat fraud in both instances may be the solution, tied to heightened mandatory minimum standards for registration and verification processes.

Aequus believes that CA training is of utmost importance in identifying potentially fraudulent calls so that CA supervisors can be alerted and appropriate preventive measures taken, including blockage of future calls and deactivation of ten-digit numbers. Aequus believes that the Commission should establish minimum standards for such preventive measures, including participation in the proposed centralized database.

V. Verification and Eligibility

While Aequus is supportive of a central database to combat IP Relay waste, fraud and abuse, this would be only as good as the data itself. That is, user data must undergo rigorous screening by providers prior to provisioning to the central database. The Commission requests what types of documentation – other than what is currently used – could be used to evaluate the eligibility of IP Relay applicants. The focus should be on how providers register – and verify – applicants, not the documentation per se, and on how providers can lawfully intervene in the midst of handling calls that give rise to flags or are of a clearly fraudulent nature. This becomes particularly problematic when handling dial around IP Relay calls by users registered with but not properly vetted by other providers.

VI. Temporary Authorization to Place Calls

Aequus strongly believes that the Commission should prohibit all IP Relay calls except those of an emergency (9-1-1) nature while verification of the applicant's registration is taking place.

VII. Revalidation of Currently Registered Users

Aequus supports revalidation of currently registered IP Relay users on an annual basis (or other time period established by the Commission). Provider costs associated with revalidation activities should be recovered through iTRS Fund rate-setting processes.

VIII. Handling of Fraudulent Calls

Aequus believes that IP Relay providers, through compliance with mandatory minimum standards, have an obligation to protect the integrity of the iTRS Fund against waste, fraud and abuse. Let us suppose a given provider through their CA notifies a merchant of a potential fraudulent call, and if the merchant determines that the call should proceed, the provider then would bill the Fund for a potentially

fraudulent call. This, of course, is not the way the Commission should go, and this would need to be weighed against the legitimate needs of validated IP Relay users to freely make calls without incurring the subjectivity of CAs who may falsely assume they are making calls of a fraudulent nature. It would therefore make sense for IP Relay providers to work with the Commission as a group to identify fraudulent call types and patterns, check such against the centralized fraud database, and point IP Relay users and merchants alike to Commission outreach and education materials aimed at combating misuse.

IX. Identification of Fraudulent Calls

Aequus believes that fraudulent IP Relay calls associated with U.S.-based IP addresses are typically the result of corrupted or "zombie" computers manipulated by users outside of or within the U.S., with ties to overseas users. It is not always possible to identify such calls before these are connected to a provider's network. Once such calls arrive, common Internet tools would typically be used to look up registration information on flagged IP addresses; if these were previously flagged for fraud or are found to originate with anonymizers, then such IP addresses are automatically blocked. There are many more ways to identify and block incoming calls of a fraudulent nature, however, the first step in combating misuse starts with more stringent verification processes to confirm legitimate applicants who wish to use IP Relay services.

X. Identification of Fraudulent Calls

Aequus believes that the Commission should utilize typical call detail for identification of fraudulent calls, with the addition of the ID of the CA or supervisor who makes the decision to disconnect the call, and the fraud category assigned based on call detail, content and/or pattern.

XI. User Authentication Methods

Aequus reiterates its strong stance with respect to more rigorous IP Relay registration processes, including heightened validation efforts by providers. Laxity in this regard has led to fraudulent user practices at the expense of legitimate users, and in turn, opportunity for IP Relay providers themselves to commit fraud by billing the iTRS Fund. Dial-around does not require anything more than registered ten-

digit numbers, with the understanding that providers who issue such numbers take appropriate authentication processes to validate IP Relay users.

XII. Dial Around

Aequus is of the opinion that the dial-around feature is both necessary and desirable for IP Relay users in the event they may be unable to reach or connect with their default provider – particularly in emergency situations. With heightened Commission requirements (and enforcement of such) for provider verification of IP Relay applicants, the dial-around feature should not contribute to relay misuse.

XIII. Central Database of Barred Users/Blocked Data

Aequus supports the concept of a central database of barred users and blocked numbers/addresses that can be populated as well as accessed by all providers, in compliance with Commission rules adopted for this purpose. Such a database can be an extension of the current iTRS database administered by Neustar. Dispute resolution in the event of provider differences of opinion on any given user in the barred/blocked database and enforcement of such, of course, would be under the purview of the Commission.

XIV. Extent of Fraud or Misuse

Aequus believes that Commission rulemaking and related efforts in recent years have contributed immeasurably toward reduction of fraud and abuse, in addition to the individual efforts of providers to combat such. What remains is adoption of more stringent IP Relay rules, including clearly articulated prohibitions and penalties for provider non-compliance. As to types of fraud committed, such can best be explained through Commission meetings with providers either individually or as a group.

XV. Additional Audit Procedures

Aequus supports any and all Commission audit procedures – including enforcement – aimed at identification and reduction of IP Relay misuse, including audit of provider registration and verification processes.

XVI. Alternatives to IP Relay

Aequus knows IP Relay is here to stay for quite some time. Text and other forms of electronic messaging, while appropriate for some situations, cannot replace telecommunications of a confidential or sensitive nature – financial transactions, as an example. IP Relay usage is not restricted to individuals who do not know American Sign Language ("ASL"). In fact, ASL users do make use of IP Relay when in situations where bandwidth is insufficient to support Video Relay Service ("VRS") communications or when they simply do not wish to be visible to the CA handling their call.

XVII. Location of Call Centers

Aequus believes that the Commission should require that all IP Relay call centers (including VRS call centers) be located within the geographic boundaries of the U.S. thereby allowing for scheduled and impromptu Commission on site visits, which would enable greater federal authority in the event of criminal activity or the commission of such.

XVIII. Conclusion

Aequus commends the Commission on taking up this important proceeding and trusts that it will take appropriate steps to combat IP Relay misuse through heightened mandatory minimum standards for registration and verification processes, greater audit and enforcement oversight, with tie-in to certification requirements and eligibility for participation in the iTRS Fund.

Respectfully submitted,

/s/
Nancy J. Bloch
Chief Regulatory and Compliance Officer
Snap Telecommunications, Inc.
On Behalf of Aequus Technologies Corporation
Two Blue Hill Plaza, Third Floor
Pearl River, New York 10965

March 20, 2012