InCharge Systems Inc.
1128 20th ST, West Des Moines, IA 50265

VIA ECFS

February 23, 2012

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W., Room TW-A325
Washington, D.C. 20554.

Re: **WC Docket Nos. 10-90, 07-135, 05-337, 03-109, CC Docket No. 01-92, 96-45, and GN Docket 09-51.**

Dear Ms. Dortch:

InCharge Systems ("ICS") hereby submits these comments in response to the above referenced proceedings and to certain comments made to them. In these proceedings, the Commission seeks comment on issues presented in the *USF/ICC Transformation Order and Further Notice of Proposed Rulemaking*[1] where the record was insufficient.

As part of the *Order* the Commission adopted new call signaling rules to address "phantom traffic."[2] Service providers that originate interstate or intrastate traffic on the PSTN, or that originate inter or intrastate interconnected VoIP traffic destined for the PSTN, are now required to transmit the telephone number associated with the calling party to the next provider in the call path. Intermediate providers must pass calling party number (CPN) or charge number (CN) signaling information they receive from other providers unaltered, to subsequent providers in the call path. The *Order* further makes clear that the CN will not contain or be populated with a number associated with an intermediate switch, platform, gateway, or other number.

We generally agree with Verizon and others who suggest it makes little sense for providers to make extensive new investments in old signaling technology and facilities given the transition away from these technologies. *Full switch replacement for the sole purpose of compliance with the new signaling rules presents an extreme burden.*[3]

By the same token, ICS agrees with the National Exchange Carrier Association (NECA) and its co-petitioners who suggest, given time to implement, it would *not appear to be unduly burdensome* to reprogram legacy switches to include a valid CN for originating traffic.[4]

---

[1] http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0206/FCC-11-161A1.pdf
[2] *See* 47 C.F.R. § 64.1601(a)(1)-(2) (the "phantom traffic rules"); *Connect America Fund, et al.*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket Nos. 10-90 *et al.*, FCC 11-161 (Nov. 18, 2011) ("*USF/ICC Transformation Order*").
[3] http://apps.fcc.gov/ecfs/comment/view?id=6016985277
[4] http://apps.fcc.gov/ecfs/comment/view?id=6016984731

We strongly agree with those commenters (e.g., Verizon) who state the lack of standardized signaling for IP traffic inhibits CPN/CN information from being passed in a format that can be processed by downstream providers. More importantly, until there are industry standards for passing such signaling information, this problem will only become more pronounced. As new technologies emerge and the number of possible call flow route permutations increase, phantom traffic disputes will logically continue to grow. [5]

The Commission needs to do everything in its power now to help standards bodies bring this issue to conclusion.

This issue could be compared to the email issues encountered by various industry committees/standards bodies in the 90's, when the European government-backed X.400 standard was dueling with Internet protocols for email. The former is quite secure, but the latter was easier to use. The industry could have harmonized them and built authentication into Internet email standards – a committee was formed to do just that - but it became a political battle and didn't happen, condemning us to a world of Nigerian princes, male-enhancement creams and nasty viruses. It didn't have to happen and was truly a costly missed opportunity. The opportunity to "get it right" presents itself once again.

ICS believes the primary reason for altering call identifying information as we transition to all IP is not to game the system, but rather to accommodate the many non-standard protocols and formats that are being utilized by different providers. It is this situation that needs more proactive Commission involvement. A standard mechanism/marker that could be verified by intermediate carriers, many times the third or fourth carrier in the chain, could be extremely beneficial.

We agree with Hypercube when they state originating carriers are the ones with the most complete, accurate information and are the most logical choice to be held accountable for compliance with the call signaling rules.[6] The Commission concluded in the *Order* that imposing any upstream liability on tandem transit and other intermediate providers may be an unfair burden. ICS agrees. Said simply, we think the onus to provide error free, verifiable data rests with the originating provider.

ICS believes resolving standards issues needs to be done first to avoid problems associated with altered or manipulated or missing signaling data. Let us not repeat the same mistakes endemic to the SS7 today, namely no agreed upon single data element or enforceable, do-not-modify marker. Until carriers, VoIP providers and equipment manufacturers agree on the relevant data and how it is exchanged, compliance efforts will have diminished utility and are arguably a needless expense continued to be borne by the public.

One would think with the implementation of the rules in this *Order* December 29, 2011 governing phantom traffic coupled with the passage of the Truth in Caller ID Act in December of 2010, the problem of traffic arriving for termination with insufficient or inaccurate identifying information would be improving.

---

[5] http://apps.fcc.gov/ecfs/comment/view?id=6016985277
[6] http://apps.fcc.gov/ecfs/comment/view?id=6016984908

It is not. Much of the misbehavior occurs when traffic is simply "laundered" through an intermediate provider who populates or repopulates the CN field with an incorrect number. An approach *that would enable a terminating provider to identify calling party information which had not been altered* would be very beneficial. Notably these are the exact words the Commission used in its Report to Congress dated June 21, 2011 in a related proceeding entitled "Caller Identification Information in Successor or Replacement Technologies."[7]

In our FCC NPRM submittal in the aforementioned proceeding,[8] we suggested adoption of an existing standards-based technological solution that enables relying parties to know if the received caller ID information has been manipulated would be the best approach. This solution relies on assigning a cryptographic signature as part of the originating call request. Further, this digital signature can authenticate an originator's caller ID information, and can be validated anywhere along the call path, including by the recipient of the call, as well as by transport or terminating network providers.

When submitting its Report to Congress, the FCC cited this "digital signature" solution in paragraphs 43 and 44 as an industry-consensus solution for authenticating caller ID, very similar to methods we use today to authenticate web sites or emails. Equally as important, the Commission went on to say the solution, if deployed, could be valuable for law enforcement and public safety purposes as well. Its use could transcend well beyond the phantom traffic mitigation value associated with the reform objectives of this *Order*.

InCharge Systems believes the current proceedings offer the Commission a unique opportunity to mandate adoption of the type of cryptographic solution mentioned above.

Thank you.

Respectfully submitted,

/s/ Michael D. Hamilton

Michael D. Hamilton, President
InCharge Systems, Inc.
1128 20th Street
West Des Moines, Iowa 50265
mikehamilton@inchargesys.com
+1.515.224.9600

[7] http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.doc
[8] http://apps.fcc.gov/ecfs/document/view?id=7021237895