

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

In the Matter of:	)	
	)	
Implementation of the Telecommunications Act of 1996;	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36

**COMMENTS OF  
ALEXICON TELECOMMUNICATIONS CONSULTING**

**I. GENERAL**

Alexicon Telecommunications Consulting (“Alexicon”) hereby submits its Comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) Further Notice of Proposed Rulemaking (“FNPRM”) in the above captioned matters adopted March 13, 2007 and released April 2, 2007<sup>1</sup>. In this FNPRM the FCC requests Comments on whether the Commission should act to expand its CPNI rules further and whether it should expand consumer protections to ensure that customer information and CPNI are protected in the context of mobile communication devices<sup>2</sup>.

Alexicon provides management, financial and regulatory consulting services to a range of small rate-of-return Incumbent Local Exchange Carriers (“ILECs”)<sup>3</sup>. These ILECs provide a variety of telecommunications services ranging from Basic Exchange Access

---

<sup>1</sup> FCC 07-22

<sup>2</sup> Order, para. 67

<sup>3</sup> As defined by the 1996 Telecommunications Act; each providing local exchange access service(s) to less than fifty thousand (50,000) access lines

Service to Advanced Telecommunications Services, including Broadband/Internet Access and similar services.

Alexicon and its client companies have been active participants in these subject (and related) Dockets, including filing of Comments in April 2006 directed at the FCC's Notice of Proposed Rulemaking in FCC 06-10. Alexicon and its clients have consistently advocated for *reasonable and cost-effective* protection of CPNI information. As ILECs, Alexicon's clients have diligently complied with FCC Rules and Regulations and believe that the "pretexting" actions<sup>4</sup> that have been the focus of previous FCC CPNI concerns<sup>5</sup> (and the EPIC petition) have generally been adequately dealt with under the revised FCC Rules contained in the current subject Order. At the present time, we advocate that the FCC not adopt further CPNI Rules and allow the revised Rules to be implemented and judged in a reasonable timeframe *before* any additional revisions are proposed/implemented.

## II. SPECIFIC COMMENTS

**A. Should password protection be extended to non-call detail? For all non-call detail, or should it include certain account changes? Would requiring these forms of password protection place an undue burden on carriers, customers, or others, including any burdens placed on small carriers?<sup>6</sup>**

Alexicon does not support further extension of the use of password protection beyond that contained in the current Order. Any password extension would cause additional expense(s) and ongoing administration costs to small carriers. As previously noted, Alexicon does not believe that small carriers need to add password protection to CPNI, as in most cases they are aware of their customers, including those customers' CPNI valid requests, versus pretexting actions.

---

<sup>4</sup> When non-customers pretend to be the customer to illegally obtain CPNI information via the customers' telecommunications carrier

<sup>5</sup> And related Congressional scrutiny

<sup>6</sup> Order, para. 68

**B. Are audit trails generally used by carriers to track customer contact? What are the burdens on small carriers to recording the disclosure of CPNI and customer contact? Would audit trails assist law enforcement with its criminal investigations against pretexters? Has technology changed such that audit trails are now an economically feasible option?<sup>7</sup>**

The maintenance of audit trail information generally requires some form of an interactive data system for use with all customer contacts (telephonic, mail, email, in-person, etc). Most smaller ILECs do not utilize such high-level interactive data systems to currently track all customer contacts. Alexicon rejects requiring small carriers to immediately expend significant monies to implement such systems. While there is probably some benefit to law enforcement agencies of audits trails, we submit that there has historically been (and there is little future probability of) significant pretexting in small ILEC areas as to require the expenditures to implement additional audit trails for small carriers for these uses.

**C. What physical safeguards are carriers currently using when they transfer, or allow access to, CPNI to ensure they maintain the security and confidentiality of CPNI? Are these safeguards sufficient? What steps should the FCC require a carrier to protect CPNI when it is being transferred or accessed by the carrier, its affiliates or its third party? What are the benefits and burdens on small carriers of requiring carriers to physically safeguard the security and confidentiality of CPNI?<sup>8</sup>**

Alexicon asserts that based on historical evidence (or the lack thereof), small ILECs do not currently have any CPNI transfer safeguard concerns. Current methods, customer-contact personnel procedures, and in-house training do not appear to be causing physical transfer problems affecting CPNI. To require new, additional or some “standard” procedures for the physical transfer of CPNI would appear to be onerous, costly and not needed for small carriers. Alexicon believes that specific individual company corrective actions could be implemented if, or when, any physical transfer CPNI issues arise.

---

<sup>7</sup> Order, para. 69

<sup>8</sup> Order, para. 70

**D. Should the FCC require carriers to limit data retention? If so, what should the maximum time of data retention be? Should the Commission define exceptions where a carrier is permitted to retain certain records? Are there state or Commission data retention requirements that might conflict with a carrier's data retention? Does a limitation on data retention enhance protection of CPNI?<sup>9</sup>**

Alexicon does not believe that data retention limitation would enhance CPNI protection. CPNI data has a limited life to other than the customer, and pretexters generally try to obtain current CPNI information. Law enforcement and civil litigants are most likely to ask for non-current CPNI in the course of their activities. Limitations of data retention may be anti-productive in these instances. Again, absent showing(s) that specific data retention periods have been non-protective of CPNI, Alexicon can see no benefit to additional data retention rules. Furthermore, there are a variety of state, federal, NECA and other data retention rules and regulations that could easily conflict with any new FCC-ordered data retention rules. Alexicon believes that burdens of new data retention rules could very likely outweigh any potential benefits to small carriers.

**E. What steps should the Commission take, if any, to secure the privacy of customer information stored in mobile communications devices? What methods do carriers currently use, if any, for erasing customer information prior to refurbishing the equipment? Should the Commission require manufacturers to configure wireless devices so consumers can easily and permanently delete personal information from those devices?<sup>10</sup>**

Alexicon's clients are neither manufacturers of mobile devices nor do they provide such devices on a regulated basis. Alexicon believes that consumers must take personal responsibility for protection of any personal information they may store in mobile communications devices. It should not be the role of the FCC to "protect consumers from themselves" in all situations. Consumers must take responsibility for CPNI protection of personal information when they have control of this information. Carriers, manufacturers, agents, or others should not bear responsibility for consumer self-

---

<sup>9</sup> Order, para. 71

<sup>10</sup> Order, para. 72

protection. We believe that current mobile communications devices are adequately configured to allow consumers to delete personal information prior to returning these devices to recyclers or others and accordingly no FCC intervention is warranted.

### **III. SUMMARY**

Alexicon appreciates this opportunity to provide its Comments in this matter. We commend the FCC for its ongoing concerns regarding the protection of CPNI. We do believe that current (including recently enhanced) CPNI rules adequately protect CPNI and the consumers who rely upon carriers to protect it. While we share the Commission's and Congressional concerns regarding the pretexting issue, it appears that this was mainly a "passing" concern that currently appears to be greatly diminished. Even when pretexting was somewhat prevalent, it appeared that smaller ILECs were not the subject of extensive attempted CPNI breaching or successful CPNI extraction by pretexters.

Alexicon respectfully suggests that the FCC allow sufficient time for the newly revised CPNI protection rules to be in effect prior to proposing revisions or additions. We suggest that the revised rules be in effect for at least one (1) year before further modifications are proposed and therefore do not support any further changes at this time.

Respectfully Submitted,

**Alexicon Telecommunications Consulting**  
**2055 Anglo Drive, Suite 201**  
**Colorado Springs, CO 80918**