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

REPLY COMMENTS OF SOUTHERNLINC WIRELESS

Southern Communications Services, Inc. d/b/a SouthernLINC Wireless ("SourthernLINC Wireless") hereby submits these reply comments in the above-captioned docket.[1] SouthernLINC Wireless operates a commercial digital 800 MHz ESMR system using Motorola's proprietary Integrated Digital Enhanced Network (iDEN) technology to provide dispatch, interconnected voice, Internet access, and data transmission services over mobile phone handsets. SouthernLINC Wireless is licensed by the Commission to provide cellular communications services in Alabama, Florida, Georgia, and Mississippi, where it serves nearly 300,000 subscribers over 127,000 square miles. SouthernLINC Wireless offers the most comprehensive geographic coverage of any mobile wireless provider in Alabama and Georgia, servicing extensive rural territory along with major metropolitan areas and highway corridors, and as such is widely used by local and statewide governmental institutions, public utilities and emergency services.

---

1 In the Matter of High-Cost Universal Service Support; Federal State Joint Board on Universal Service, *Notice of Proposed Rulemaking*, FCC 07-88 (rel. May 14, 2007) ("*USF Cap NPRM*").

SouthernLINC Wireless is committed to offering high-quality telecommunications services to rural and underserved areas and to protecting the confidential information of its subscribers, including their Customer Proprietary Network Information ("CPNI"). As such, SouthernLINC Wireless supports the goals that led the Commission to adopt additional measures in the recent CPNI Order to safeguard customers' personal information from pretexters, in fulfillment of the congressional mandate in section 222(a) of the Act.[2] However, SouthernLINC Wireless also agrees with the overwhelming majority of parties who commented in this proceeding that additional CPNI rules are not necessary at this time.[3] Additional CPNI rules could harm both customers and carriers without improving the safety of the confidential information of the customers, as explained in more detail below.

I. THE COMMISSION SHOULD NOT ADOPT ADDITIONAL CPNI RULES AT THIS TIME

SouthernLINC Wireless agrees with the overwhelming majority of commenters that the Commission should not adopt additional password requirements at this time.[4] The burdens of additional password requirements far outweigh any benefits, particularly since there is no record evidence to suggest that the rules the Commission adopted in the CPNI Order are

---

2 47 U.S.C. § 222(a).

3 *See, e.g.* ,Comments of the AAPC; Comments of Alexicon; Comments of AT&T; Comments of Comcast; Comments of CompTel; Comments of Embarq; Comments of Frontier; Comments of the ITTA; Comments of the Iowa Telecommunications Association ("ITA"); Comments of MetroPCS; Comments of the NCTA; Comments of the NTCA; Comments of Nuvox and XO; Comments of Qwest; Comments of RCA; Comments of Sprint Nextel; Comments of T-Mobile; Comments of Time Warner; Comments of USA Mobility; Comments of USTelecom; Comments of Verizon.

4 *See, e.g.* , Comments of Alexicon of 2; Comments of AT&T at 2-8; Comments of Comcast at 4-6; Comments of CompTel at 2-3; Comments of Embarq at 3; Comments of Frontier at 2-5; Comments of the ITA at 3-4; Comments of the ITTA at 2-3; Comments of Metro PCS at 2-6; Comments of the NCTA at 2-3; Comments of the NTCA at 2-3; Comments of Nuvox and XO at 2-5; Comments of Qwest at 5-7; Comments of RCA at 2-3; Comments of Sprint Nextel at 2-10; Comments of T-Mobile at 2-3; Comments of Time Warner at 3-8; Comments of USA Mobility at 3-8; Comments of USTelecom at 3-4; Comments of Verizon at 3-10.

insufficient to protect customers.[5] As Verizon and others correctly observed, no compelling evidence has arisen in the three months since the release of the CPNI Order that would support a reversal of course to extend the password requirements.[6] Requiring a customer to provide a password before a customer service representative could provide any CPNI over the telephone would be frustrating to customers and unnecessarily burdensome.[7] To many customers, the added security benefit of requiring the submission of a customer-set password before any CPNI could be released would come at too great a cost in terms of lost efficiency and convenience in conducting legitimate account transactions.[8]

Verizon is also correct that password requirements for the disclosure of CPNI would violate the First Amendment.[9] Additional password requirements would unnecessarily restrict customers' ability to obtain information they want from their service provider and carriers' ability to provide information they wish to provide.[10]

---

5 *See, e.g.,* Comments of Alexicon of 2; Comments of Comcast at 4-6; Comments of Embarq at 3; Comments of Frontier at 3-5; Comments of the ITA at 3-4; Comments of Metro PCS at 2-6; Comments of the NCTA at 2-3; Comments of the NTCA at 2-3; Comments of Nuvox and XO at 4-5; Comments of Qwest at 5-7; Comments of RCA at 2-3; Comments of Sprint Nextel at 6-10; Comments of T-Mobile at 2-3; Comments of Time Warner at 3-8; Comments of USA Mobility at 3-8; Comments of Verizon at 3-10.

6 *See, e.g.,* Comments of Alexicon of 2; Comments of AT&T at 2-8; Comments of Embarq at 3; Comments of Frontier at 3-5; Comments of the NCTA at 2-3; Comments of Nuvox and XO at 4-5; Comments of Verizon at 3.

7 *See* Comments of Verizon at 3-4(providing examples where password restrictions would be unnecessarily burdensome); *see also, e.g.,* Comments of Comcast at 4-6; Comments of Embarq at 3; Comments of Frontier at 3-5; Comments of the ITA at 3-4; Comments of the ITTA at 2-3; Comments of the NCTA at 2-3; Comments of Nuvox and XO at 3-4; Comments of Qwest at 5-7; Comments of RCA at 2-3; Comments of T-Mobile at 2-3; Comments of USTelecom at 3-4.

8 *See, e.g.,* Comments of Comcast at 4-6; Comments of Embarq at 3; Comments of Frontier at 3-5; Comments of the ITA at 3-4; Comments of the ITTA at 2-3; Comments of the NCTA at 2-3; Comments of Nuvox and XO at 3-4; Comments of Qwest at 5-7; Comments of RCA at 2-3; Comments of T-Mobile at 2-3; Comments of USTelecom at 3-4; Comments of Verizon at 4-7.

9 *See, e.g.,* Comments of Verizon at 10-11.

10 *See, e.g.,* Comments of Verizon at 10-11.

SouthernLINC Wireless agrees with the majority of commenters that audit trails are of extremely limited value in fighting pretexting, and a requirement that carriers create and maintain audit trails would force carriers to generate excessive data to respond to legitimate customers inquiries.[11] Indeed, nothing relevant has changed since the Commission twice rejected a requirement to keep an audit trail of all CPNI disclosures.[12] In any event, under the new password/backup authentication and customer notification requirements, audit trails will not be necessary.

The rules the Commission adopted in the CPNI Order and the criminalization of pretexting alleviate the need for additional physical safeguards.[13] Moreover, pretexters generally have relied upon simple theft or low-tech ruses designed to bypass authentication procedures rather than "high-tech" methods of infiltrating carrier networks.[14] Accordingly, there is no evidence on the record in this proceeding to suggest that rules imposing additional physical safeguards are necessary to protect CPNI.[15]

---

11 *See, e.g.,* Comments of Alexicon of 3; Comments of Comcast at 6-7; Comments of Embarq at 3; Comments of the ITA at 4-5; Comments of the ITTA at 3-4; Comments of Metro PCS at 7-8; Comments of the NCTA at 3-4; Comments of Nuvox and XO at 5-6; Comments of Qwest at 8-11; Comments of RCA at 3-4; Comments of Sprint Nextel at 10-12; Comments of T-Mobile at 4-6; Comments of Time Warner at 9-10; Comments of USA Mobility at 9-10; Comments of USTelecom at 4-5.

12 *See, e.g.,* Comments of Comcast at 6-7; Comments of the NCTA at 3-4; Comments of Nuvox and XO at 6; Comments of Qwest at 8; Comments of T-Mobile at 4-6; Comments of Verizon at 11-15.

13 *See, e.g.,* Comments of Alexicon of 3; Comments of Comcast at 8; Comments of the ITTA at 4-5; Comments of Metro PCS at 8-10; Comments of Nuvox and XO at 6-7; Comments of Qwest at 11-12; Comments of RCA at 4-5; Comments of Sprint Nextel at 12-14; Comments of T-Mobile at 6; Comments of Time Warner at 10-11; Comments of USA Mobility at 10-11; Comments of USTelecom at 5; Comments of Verizon at 15-17.

14 *See, e.g.,* Comments of Comcast at 8; Comments of Sprint Nextel at 14; Comments of T-Mobile at 6; Comments of Time Warner at 10-11; Comments of USA Mobility at 10-11.

15 *See, e.g.,* Comments of Alexicon of 3; Comments of Comcast at 8; Comments of Embarq at 4-5; Comments of the ITA at 5-6; Comments of the ITTA at 3-4; Comments of Metro PCS at 9-10; Comments of Nuvox and XO at 6-7; Comments of Qwest at 11-12; Comments of T-Mobile at 6; Comments of USTelecom at 5.

The record demonstrates that the Commission should not establish new rules limiting CPNI data retention.[16] Limiting data retention will not reduce pretexting and, thus, is unnecessary.[17] Moreover, limiting data retention will create unnecessary conflicts among various federal and state statutory limitations periods.[18]

SouthernLINC Wireless also agrees with commenters who observe that "customer information" stored in handsets is neither CPNI nor proprietary information protected under section 222 of the Act.[19] Moreover, additional rules are unnecessary because carriers already delete customer information from handsets that are returned for recycling.[20] However, since not all handsets are returned to carriers, carriers are not in the position to guarantee the security of information on handsets, and thus the Commission should not impose rules placing this responsibility on carriers.[21] SouthernLINC Wireless agrees with Verizon that carriers require

---

16 *See, e.g.,* Comments of Alexicon of 4; Comments of Comcast at 8-9; Comments of Embarq at 4; Comments of the ITA at 6; Comments of Metro PCS at 10-11; Comments of Nuvox and XO at 7-8; Comments of Qwest at 13-15; Comments of RCA at 5-6; Comments of Sprint Nextel at 14-19; Comments of T-Mobile at 7; Comments of Time Warner at 11-12; Comments of USA Mobility at 11-12; Comments of USTelecom at 6; Comments of Verizon at 17-20.

17 *See, e.g.,* Comments of Alexicon of 4; Comments of Comcast at 8-10; Comments of the ITA at 6; Comments of Metro PCS at 10-11; Comments of RCA at 5-6; Comments of Sprint Nextel at 16-17; Comments of Time Warner at 11-12; Comments of USA Mobility at 11-12; Comments of Verizon at 17-20.

18 *See, e.g.,* Comments of Embarq at 4; Comments of Nuvox and XO at 7-8; Comments of Sprint Nextel at 17-19; Comments of T-Mobile at 7; Comments of USTelecom at 6; Comments of Verizon at 17-20.

19 *See, e.g.,* Comments of Sprint Nextel at 20-22.

20 *See, e.g.,* Comments of Alexicon of 4-5; Comments of Embarq at 5; Comments of Sprint Nextel at 22-23; Comments of Qwest at 15-16; Comments of RCA at 6-7; Comments of T-Mobile at 8; Comments of Time Warner at 9-10; Comments of USA Mobility at 9-10.

21 *See, e.g.,* Comments of the ITA at 7; Comments of Metro PCS at 11-12; Comments of Qwest at 15-16; Comments of RCA at 6-7; Comments of Sprint Nextel at 23-24.

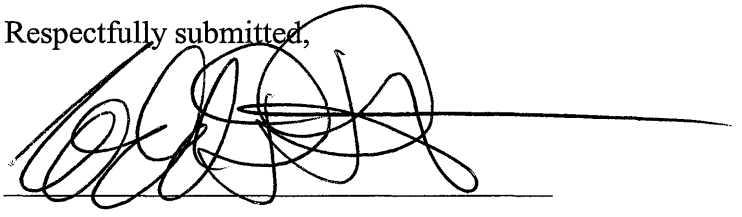
flexibility in their data retention practices to meet a variety of objectives and legal requirements, including the protection of CPNI.[22]

Finally, SouthernLINC Wireless agrees that the Commission should not adopt any new measures designed to protect residential customer data, or extend any such requirements to business customers.[23] Customers, particularly sophisticated business customers, should have the right to negotiate authentication and CPNI protection measures that best serve their needs.

II. CONCLUSION

For the reasons set forth above, SouthernLINC Wireless urges the Commission not to adopt any additional CPNI rules at this time.

Respectfully submitted,



Michael D. Rosenthal
Director of Legal and External Affairs
Holly Henderson
External Affairs Manager
SouthernLINC Wireless
5555 Glenridge Connector, Suite 500
Atlanta, GA 30342
T: (687) 443-1500

Todd D. Daubert
Kelley Drye & Warren LLP
Washington Harbour, Suite 400
3050 K Street, NW
Washington, DC 20007-5108
T: (202) 342-8400
F: (202) 342-8451
tdaubert@kelleydrye.com

Counsel for SouthernLINC Wireless

22 *See, e.g.,* Comments of Verizon at 17-20.

23 *See, e.g.,* Comments of USTelecom at 6; Comments of Verizon at 20-21.