



Sprint Nextel
2001 Edmund Halley Drive
Reston, VA 20191
Office: (703) 592-5113 Fax: (703) 592-7404

Luisa L. Lancetti
Vice President
Government Affairs – Wireless

November 21, 2006

Via Electronic Submission

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

***Re: Notice of Ex Parte Communication
CC Docket No. 96-115; RM 11277***

Dear Ms. Dortch:

This letter is to inform you that on November 20, 2006, Kent Nakamura, Luisa Lancetti and Frank Triveri of Sprint Nextel Corporation (“Sprint Nextel”) met with Barry Ohlson (Senior Legal Advisor for Spectrum and International Issues) and Scott Bergmann (Legal Advisor for Wireline Issues) of Commissioner Jonathan Adelstein’s office, to discuss the Commission’s *Notice of Proposed Rulemaking* in the above-referenced proceedings and the steps that Sprint Nextel is taking to safeguard Customer Propriety Network Information. The attached material was discussed and distributed at the meeting.

Pursuant to Section 1.1206 of the Commission’s rules, this letter is being electronically filed with your office. Please associate this letter with the file in the above-referenced proceedings.

Respectfully submitted,

/s/ Luisa L. Lancetti
Luisa L. Lancetti

Attachment

cc: Michelle Carey
John Hunter
Bruce Gottlieb
Ian Dillner
Barry Ohlson
Scott Bergmann
William Dever
Jonathan Reel
Cindy Spiers
Timothy Stelzig

CUSTOMER PROPRIETARY NETWORK INFORMATION RULEMAKING
Docket No. 96-115

Sprint Nextel Ex Parte Presentation
October 31, 2006

Sprint Nextel supports the goal of the Commission's rulemaking: to ensure the safeguarding of customer proprietary network information (CPNI). Sprint Nextel believes that carriers, together with the Commission, must protect customers against threats to privacy; and that those who breach security to illegally obtain CPNI must be held accountable.

Sprint Nextel's Implementation of Privacy and Information Safeguards

Sprint Nextel has addressed threats to privacy and information security as follows:

- Technical safeguards for the wireless customer-service platform: Since early 2006, Sprint Nextel has been planning systems-based improvements to enhance authentication and information security. Sprint Nextel selected a new platform to unify pre-merger wireless billing and customer-service platforms. Sprint Nextel's new wireless customer-service platform will significantly enhance authentication capabilities. Sprint Nextel has dedicated a large amount of resources at great expense. Sprint Nextel expects to start deployment of these upgraded authentication capabilities in 2007. Planned or existing capabilities include:
 - Phased elimination of social security number as an authenticator.
 - Phased implementation of passwords and shared secrets: The customer will select a password and a shared secret (e.g., what was your first pet's name?).
 - Optional auto-generated notification: Sprint Nextel expects to notify the customer of account changes and confirm requests for call-detail information.
 - Audit trails: Sprint Nextel will enhance its current audit-tracking capabilities to show all instances where customer service representatives view customer records.

For long-distance customers, Sprint Nextel will first improve procedures to enhance authentication. System improvement changes, similar to wireless, will be considered upon completion of wireless customer service platform enhancements.

- Training: Sprint Nextel uses formal training programs, bulletins, and alerts to train employees on authentication and security procedures.
- Testing and Auditing: Sprint Nextel conducted a privacy assessment and audit of its authentication and customer information security regime. As part of its privacy compliance effort, Sprint Nextel expects to continue testing and auditing, and use the results to improve authentication and information security.

- Reporting and adjustment: Sprint Nextel's internal reporting procedures and mechanisms are being reviewed and improved to alert compliance personnel of possible breaches that warrant adjustments in safeguards.

CPNI Safe-Harbor Safeguards Must Be Dynamic to Change with the Times

- Sprint Nextel endorses a Safe-Harbor standard modeled after the privacy and information security provisions of the Gramm-Leach-Bliley Act (GLBA)—the law that governs financial institutions. GLBA safeguards are used to safeguard the most sensitive information: personal financial information.
- The GLBA uses an analytical framework, requiring covered entities to use due diligence to assess and address threats to privacy and information security. In general, the GLBA requires financial institutions to assess risks, implement solutions to mitigate those risks, train employees, test compliance, adjust where necessary, and repeat the process. The safeguards change with the times to better protect customer information.
- Sprint Nextel is in the process of implementing a GLBA-like compliance program. Governing industry standards bodies and organizations—e.g., ISO/IEC information security standard, SAS-70 audit standard, the credit card payment card industry (“PCI”) standard, and the Federal Government’s GLBA—favor such standards-based approaches to information security. They recognize that no one prescriptive measure works best, and that flexibility is needed to meet emerging threats.

Conclusion: Sprint Nextel’s Approach Addresses Immediate and Future Threats

- Sprint Nextel’s overall approach to authentication and information security, which is being modeled on the GLBA, is designed to address immediate and future harms. This approach provides the best possible protection against con artists who use low-tech means like social engineering to obtain personal information to breach security and impersonate customers.
- Sprint Nextel’s approach ensures that safeguards change over time to meet emerging threats. Overly prescriptive regulations that lock carriers into static compliance measures would prevent carriers from innovating to meet future threats. By endorsing a GLBA-like analytical framework for carriers, the Commission would achieve a dynamic regulatory solution to a serious consumer-protection issue.