March 1, 2009

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Re: Annual CPNI Compliance Certification, EB Docket No. 06-36

Dear Secretary Dortch:

Attached, for filing in EB Docket No. 06-36, is the Annual 47 C.F.R. § 64.2009(e) CPNI Compliance Certification and accompanying statement of Sprint Nextel Corporation.

If there are questions regarding this filing, please contact the undersigned. Thank you for your assistance.

Respectfully Submitted,

Edward Palmieri
Senior Counsel & Director
Sprint Nextel Corporation

cc: Federal Communications Commission
   Enforcement Bureau, Telecommunications Consumers Division
   445 12th Street, SW
   Washington, DC  20554
   (2 copies via mail)

cc: Best Copy and Printing
   (via email to  FCC@BCPIWEB.COM)

cc: Marcy Greene
   (via email to Marcy.Greene@fcc.gov)
Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Sprint Nextel Corporation

Date Filed:  March 1, 2009

Name of company covered by this certification:  Sprint Nextel Corporation

Form 499 Filer ID:

804636 – Sprint Communications
811754 – Sprint Spectrum, LP
818104 – SprintCom, Inc.
812437 – Sprint Telephony PCS, LP

819060 – Phillie Co, LP
811156 – American PCS Communications
822116 – Nextel Communications-Consolidated
819224 – Nextel Partners, Inc.

Name of Signatory: Kent Y. Nakamura
Title of signatory:  Vice President and Chief Privacy Officer

SPRINT NEXTEL CORPORATION
2008 CPNI COMPLIANCE CERTIFICATE AND STATEMENT

I, Kent Y. Nakamura, certify that I am an officer of Sprint Nextel Corporation, and that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission’s CPNI rules (see 47 C.F.R. § 64.2001 et seq).

Attached to this certification is an accompanying statement explaining how the company’s operating procedures ensure compliance with the requirements of section 64.2001 et seq. of the Commission’s rules. The statement also provides a summary of the customer complaints that the company has received in the past year concerning the unauthorized access to CPNI.

Executed on March 1, 2009.

[Signature]

Kent Nakamura
Vice President & Chief Privacy Officer
Sprint Nextel Corporation
The following statement explains the operating procedures established by Sprint Nextel Corporation and its affiliates (collectively, “Sprint Nextel” or “Company”) to ensure that it is in compliance with the Federal Communications Commission’s CPNI rules. Specifically, “Sprint Nextel” refers to all Sprint Nextel Corporation’s operating entities and divisions, including those referred to as Sprint Nextel, Sprint, Nextel, Boost¹ or Xohm.² Sprint Nextel focused this year on providing CPNI compliance training to its employees, contractors, and its indirect sales channel partners and enhancing customer authentication systems and processes, notification procedures, and CPNI complaint reporting processes. Sprint Nextel’s Office of Privacy, along with several business units, continues to monitor the Company’s systems and processes related to its enterprise-wide CPNI compliance programs. As such, Sprint Nextel will continue to update and deploy CPNI training, review and adjust where necessary its customer authentication, information security, and notification procedures, and strengthen the Company’s administrative, physical and technical safeguards.

**Safeguards**

Sprint Nextel employs administrative, physical and technical safeguards that are designed to protect CPNI from unauthorized access, use and disclosure.

Sprint Nextel limits CPNI access to employees, independent contractors and joint venture partners consistent with their job functions. If access is required, they must first obtain approval through established administrative processes. Once approval is granted, user IDs and passwords are issued. Access credentials are governed by Sprint Nextel’s Corporate Security policies, which are consistent with industry standard requirements for password management for information technology networks, applications and databases.

Before disclosing CPNI to independent contractors or joint venture partners, Sprint Nextel enters into agreements with strict privacy and confidentiality provisions that require third parties to maintain confidentiality, protect the information, and comply with the law. Sprint Nextel’s Office of Privacy continually reviews Sprint Nextel’s standard privacy-related contract terms and conditions to ensure that those provisions adequately safeguard all customer information. In negotiating and renewing its contracts, Sprint Nextel requires independent contractors and joint venture partners with which it shares CPNI to safeguard this information in a manner that is consistent with the FCC’s rules. Specifically, these contract terms require third parties with access to CPNI to have appropriate CPNI protections in place to ensure the ongoing confidentiality of such information. These provisions require securing all Sprint Nextel data; limiting access to persons who have a need-to-know such information in connection with the performance of the contract; ensuring all persons with access are bound by specified confidentiality obligations; and restricting the use of CPNI solely to the performance of the contract.

---

¹ Boost Mobile, LLC (“Boost”) is a subsidiary of Sprint Nextel Corporation and offers a lifestyle-based youth brand presently focused on offering prepaid communications products and services.

² Xohm was a new 4G business division of Sprint Nextel, with a mission to develop a better kind of wireless broadband experience. Xohm did not offer any services that implicated the CPNI rules in 2008. Xohm merged with Clearwire Corporation, another 4G company, in December of 2008 to form a new and separate company called New Clearwire Corporation.
Review and Recordkeeping for CPNI Marketing Use and Sharing

Sprint Nextel uses a marketing campaign management system for review, approval and recordkeeping for outbound marketing campaigns that involve the access, use or disclosure of CPNI. That process requires the requestor, who is internal to Sprint Nextel, to complete a form that describes the campaign and indicates whether CPNI would be shared and/or used as selection criteria for the campaign. Once the requestor has completed the form, it is submitted for review to a marketing review team that has been advised by the Office of Privacy. This team determines whether the activity includes the access, use or disclosure of CPNI. This process helps to ensure that Sprint Nextel does not use the CPNI in a way that violates the CPNI rules.

Records of all the foregoing marketing campaign activities are maintained through the use of marketing resource and project management tools. A description of the campaign and details on what products and services are offered in the campaign are maintained in Sprint Nextel’s marketing resource management tool. A flag indicating whether or not CPNI is used on a campaign and the specific types of CPNI that are used for that campaign are maintained in Sprint Nextel’s marketing campaign project tracking system.

CPNI Notice and Consent Process

Sprint Nextel uses CPNI to provide customers with the services to which they subscribe and for marketing purposes within the total service relationship. Effective May 2007, Sprint Nextel does not access, use or disclose CPNI for marketing services to which the customer does not already subscribe (i.e., cross-marketing). As such, Sprint Nextel does not send out CPNI opt-out notices. If Sprint Nextel uses CPNI for cross-marketing purposes, Sprint Nextel will first send opt-out notices or obtain the appropriate opt-in consent as required by the CPNI rules. Sprint Nextel also no longer accesses, uses or discloses CPNI for marketing of non-communications related products or services and thus does not obtain opt-in consent for those purposes.

When Sprint Nextel provides notice or obtains consent for access, use or disclosure of CPNI, these records are maintained through a variety of systems and processes. This allows employees to determine the status of a customer’s CPNI approval prior to any access, use or disclosure of CPNI that would require customer consent pursuant to the FCC’s rules.

Sprint Nextel has never provided Boost Mobile customers with a CPNI opt-out notice because Boost does not use its customers’ CPNI to cross-market other services in the manner contemplated under 47 CFR § 64.2008, thus making such notification unnecessary.

Training and Disciplinary Process

Consistent with Sprint Nextel’s commitment to preserving customers’ privacy, the Company is continuing with a variety of training programs for its employees and contractors. The training explains how Sprint Nextel employees and contractors must access, use, store, disclose and secure CPNI to ensure compliance with the FCC’s rules and Company policies. The employee completion rate for this training exceeded 90% for the year.

In 2008, Sprint Nextel expanded its CPNI training to cover its indirect sales channel partners. Sprint Nextel currently is working to include CPNI compliance training in the Company’s on-boarding process for new indirect channel dealers.
Sprint Nextel also maintains a disciplinary process as part of Company procedures that address CPNI compliance. Sprint Nextel security personnel investigate instances of potential improper access or disclosure of CPNI by employees. If the investigation indicates a violation has occurred, disciplinary action is taken, up to and including termination.

**Authentication**

In 2008, Sprint Nextel completed the consolidation of all Sprint Nextel wireless customers onto a unified billing platform (UBP). The migration to UBP was unique and complex, involving a lengthy process to ensure a positive customer experience and to avoid disruptions of services. A majority of wireless customers were migrated to the UBP in late 2007. The migration of all customers was completed in mid-2008. This migration schedule was explained to the FCC in Sprint Nextel’s Waiver Petition \(^3\) (see below under “Waiver Petition”).

Most significantly, the UBP delivers systematic features that substantially enhance customer authentication and security. Within the UBP, many Sprint Nextel wireless customers establish a Personal Identification Number (PIN) that is required for account access to sensitive customer information. In the event a UBP customer cannot recall his/her PIN, the UBP allows customers to pre-select a security question and to provide an answer to that question. UBP customers who do not have a PIN are authenticated using a password from a previous billing system, if one existed, or by several other means, such as through secure third-party verification services or by visiting a retail location and providing a valid government issued photo ID. Where appropriate and as permitted by the Commission’s rules, Sprint Nextel may work directly with a business customer through a dedicated representative to establish an authentication regime that works best for that customer. Customers are not authenticated using readily available biographical information or account information when attempting to access call detail records over the telephone or when establishing or changing their PIN.

Sprint Nextel wireless customers who wish to obtain their call detail information have several options. If contacting Sprint Nextel by telephone with their PIN, Sprint Nextel will send call-detail records to an address designated by the customer at that time. If the customer does not have a PIN or cannot provide the PIN, Sprint Nextel will send the call detail records to the customer’s “address of record,” as defined by the CPNI rules \(^4\). Customers with a valid, government issued photo-ID also may visit a Sprint Nextel retail store to establish or change his/her account PIN or to access call detail records.

For UBP wireless customers who wish to access their account online, Sprint Nextel requires all customers to establish and use a username and password. Prior to establishing an online username and password, Sprint Nextel authenticates these customers through secure third party verification systems by sending a temporary verification code to the customer’s wireless device or by requiring the customer to input his/her UBP PIN. If the customer cannot recall his/her online username or password, Sprint Nextel makes several backup methods available so that those customers can be authenticated before they retrieve their information.

---


\(^4\) Id. at ¶13 n.46; 47 C.F.R. § 2003(b).
For wireline customers, Sprint Nextel developed compliant processes to handle customers who contact Sprint Nextel via telephone. If a wireline customer requests access to his/her call detail records, Sprint Nextel will only send those records to the address confirmed with the customer via a follow-up outbound call to the customer’s “telephone number of record,” as defined by the CPNI rules. In 2008, Sprint Nextel also completed development of its online systems for accessing wireline account information, which systems authenticate in accordance with the Commission’s rules.

Notifications

Sprint Nextel provides notice to its customers when a triggering event occurs. Such events include the creation of, or change to, an account PIN, password, security question or answer, online account or address of record. These notifications are provided to customers through a variety of means, including messages to the customer’s telephone number of record, postal mail or electronic mail to the customer’s address of record, and text messages. The notification includes information to alert the customer of the underlying event, but does not disclose any of the new or changed information, in accordance with the FCC’s rules.

In the event that a breach of customer information includes CPNI, Sprint Nextel provides notice to impacted customers and law enforcement. Such notification provides customers with enough information to understand the nature of the breach, the scope of impacted information and recommendations on how the customer should respond. If the impacted customer alerts Sprint Nextel of a potential breach, Sprint Nextel investigates the customer’s allegations and communicates as necessary with the customer and/or the government.

Data Brokers

In 2007, Sprint Nextel actively supported the Federal Trade Commission’s (FTC) investigation of, and lawsuit against, a data broker. On April 26, 2006, the FTC filed suit against Accusearch, Inc., for violation of Section 5(a) of the FTC Act and 15 U.S.C. § 45(a). The FTC asserted that Accusearch was illegally obtaining and selling call detail records. Kent Nakamura, Sprint Nextel’s Vice President and Chief Privacy Officer, served as a witness for the FTC. With help from Mr. Nakamura and others, the FTC was able to build its case against Accusearch. The FTC’s request for relief was granted in late December of 2007 and Accusearch was permanently restrained and enjoined from obtaining, marketing, or selling customer phone records and consumer personal information that is derived from customer phone records without proper authorization and consent. Accusearch also was ordered to pay a fine. The FTC publicly thanked Sprint Nextel, among others, for their assistance in this lawsuit. Accusearch has appealed the decision to the United States Court of Appeals for the Tenth Circuit.

In 2008, Sprint Nextel continued to monitor for pretexting or other harmful data broker activities. Thankfully, Sprint Nextel has observed a dramatic decline in pretexting incidents. Therefore, Sprint did not institute any proceedings or file any petitions against any data broker in any state commission, the court system or the FCC in 2008. Sprint Nextel continues to deploy safeguards to protect against, mitigate and detect pretexting activities.

CPNI Complaint Reporting

Sprint Nextel’s CPNI compliance program includes processes that enable Sprint to comply with CPNI documentation and reporting obligations, including maintaining a record of notifications to, and responses from, law enforcement and customers, and the relevant dates and descriptions of the complaints. These records are maintained for a minimum of two years.

The following data is comprised of all complaints related to unauthorized access received by Sprint Nextel in 2008. Some of these complaints were submitted to Sprint Nextel directly by the complainants themselves, and some have been called to Sprint Nextel’s attention by government agencies or the Better Business Bureau.

Most of Sprint Nextel’s 2008 non-fraud related investigations revealed that complaints were connected to domestic disputes where a family member or friend impersonates the customer and gains access to the customer’s account. A review of the fraud-related cases suggests that access to CPNI is not the primary objective; rather it is likely incidental to other disputes. Sprint Nextel will continue to monitor these occurrences and make changes where necessary.

The complaints are broken down by category, as follows:

- Number of complaints of alleged unauthorized access to CPNI by a third party: 1001
- Number of complaints of alleged unauthorized access to CPNI by a Sprint employee or contractor: 474
- Number of complaints of alleged unauthorized online access to CPNI: 393

Sprint investigates all of these complaints. These investigations show that, in over 75% of the cases, there is no evidence that a CPNI violation occurred. As for the remaining cases, Sprint Nextel confirms a violation or determines that there is evidence of a violation and, out of an abundance of caution, classifies the complaint as one implicating CPNI.

In addition to the above complaints, Sprint Nextel encountered instances where it was not clear whether the type of incident would be considered a complaint under the CPNI rules (e.g., a fraud incident). For these situations, there is no specific evidence or indication that CPNI was improperly accessed because incident related to equipment theft rather than CPNI access. Out of an abundance of caution, Sprint Nextel includes these instances of fraud (and also has included these instances in Sprint Nextel’s reports to the United States Secret Service and FBI):

- Number of complaints of fraud-related incidents where equipment theft, rather than CPNI access, was the apparent primary objective: 1791
Waiver Petition

On December 3, 2007, Sprint Nextel requested a waiver of the obligations imposed on the Company pursuant to Commission Rules 64.2010 (b), (c), (e) and (f)\(^6\) that were adopted in the CPNI Report and Order.\(^7\) The waiver was necessary to allow Sprint Nextel to finish pursuing its systematic solution for CPNI compliance through the ongoing migration of its wireless customers to the UBP. The UBP automates CPNI compliance through password verification, auto-generated customer notifications, and technical security measures. Sprint Nextel completed the migration of its wireless customers to the UBP in mid 2008. In addition, Sprint Nextel completed the deployment of CPNI compliant solutions to authenticate new residential and business wireline customers when they first register for an online account and to notify them of account changes.

---

\(^{6}\) 47 C.F.R. §§ 64.2010 (b), (c), (e) and (f).