

Timolyn Henry

**ORIGINAL**

**From:** Kelly, Tamela D [LTD] [Tamela.Kelly@sprint.com]  
**Sent:** Friday, May 05, 2006 4:34 PM  
**To:** Filings@psc.state.fl.us  
**Cc:** Masterton, Susan S [LTD]  
**Subject:** Docket No. 060158-TL, Sprint-Florida, Inc. response to Commission Order No. PSC-06-0258-PAA-TL  
**Attachments:** 060158-TL, Sprint's Response regarding CPNI 5-5-06.pdf

<<060158-TL, Sprint's Response regarding CPNI 5-5-06.pdf>>

**Filed on behalf of:**  
**Susan S. Masterton**  
**Attorney**  
**Sprint - Law/External Affairs**

**Sprint**  
**1313 Blair Stone Rd.**  
**Tallahassee, FL 32301**  
**M/S FLTLHO0201**  
**Voice (850)-599-1560**  
**Fax (850)-878-0777**  
**Susan.Masterton@sprint.com**  
**Docket No: 060158-TL**

**Title of filing:** Docket No. 060158-TL, Investigation of protection of customer proprietary network information by incumbent local exchange companies.

**Filed on behalf of:** Sprint Florida, Inc.  
**No. of pages:** 24 pages  
**Description:** Sprint-Florida, Inc. response to Commission Order No. PSC-06-0258-PAA-TL, which details measures the company takes to secure its CPNI.

*Tamela D. Kelly*  
*Regulatory Affairs Assistant*  
*Office: 850 599-1029*  
*Fax: 850 878-0777*  
*tamela.kelly@sprint.com*

CMP \_\_\_\_\_  
COM \_\_\_\_\_  
CTR \_\_\_\_\_  
ECR \_\_\_\_\_  
GCL \_\_\_\_\_  
OPC \_\_\_\_\_  
RCA \_\_\_\_\_  
SCR \_\_\_\_\_  
SGA \_\_\_\_\_  
SEC   1    
OTH   5/5/2006  

DOCUMENT NUMBER-DATE  
**04020 MAY-5 06**  
FPSC-COMMISSION CLERK



ORIGINAL

Susan S. Masterton  
Attorney

Law/External Affairs

Post Office Box 2214  
1313 Blair Stone Road  
Tallahassee, FL 32316-2214  
Mailstop FLTLH00107  
Voice 850 599 1560  
Fax 850 878 0777  
susan.masterton@mail.sprint.com

May 5, 2006

Ms. Blanca Bayó, Director  
Division of Administrative Services and  
Commission Clerk  
2540 Shumard Oak Blvd.  
Tallahassee, FL 32399-0850

Re: Docket No. 060158-TL, Investigation of protection of customer proprietary network information by incumbent local exchange companies.

Dear Ms. Bayó:

In Order No. PSC-06-0258-PAA-TL, the Commission ordered each incumbent local exchange telecommunications company to file a report detailing the measures the company takes to secure its customer proprietary network information (CPNI) and to identify any additional security measures the company has implemented, including the date of implementation. In compliance with the Order, Sprint-Florida, Incorporated ("Sprint") submits the following information:

- 1. Calls to Business Office:** Under Sprint's current practices, when customers call into the business office Sprint requires identity verification by giving customers an option of: last four digits of their social security number (SSN); a preset password; or their 13-digit customer code. Sprint recognizes that even though most customers prefer the convenience of SSN, access to social security numbers by pretexters has made their use increasingly vulnerable. To address this concern, Sprint has already begun additional education of its customer service representatives to alert them to the importance of assuring that a customer is properly identified before account information is provided. Additionally, by the end of third quarter, our customer representatives will proactively encourage customers to establish a password, in lieu of using the last four digits of their social security numbers, during all customer contacts. For those customers who choose to continue using their social security numbers for identification, Sprint will implement additional protections by requiring customers to provide, in addition to the last four digits of their social security numbers, some other identifying piece of information from their bills. Implementation for all customer contacts, both business and residential, requires customer service representative training throughout the customer care organization. Sprint anticipates beginning the training in July 2006 and completing the training by September 2006 with full implementation completed by the end of third quarter 2006.

DOCUMENT NUMBER-DATE

04020 MAY-5 06

FPSC-COMMISSION CLERK

2. **On-line Registration:** Sprint's initial comments on this subject which were filed with Mr. Moses on January 19, 2006, explained that customers currently wanting on-line access were required to use their full 13-digit account number in order to complete the registration process. As an interim step, beginning in June 2006, Sprint's practices will require that when a customer initially registers for online access to the customer's bill, the customer must provide either: 1) the billing telephone number and two of the following identifiers: last four digits of the customer's social security number, billing zip code or the customer code; or 2) the 13-digit account number and either the last four digits of the social security number or the billing zip code. The customer then establishes a password within certain parameters that preclude the password from being the customer's social security number. In addition, the customer is asked to answer a "security question" to be used to reset access to the customer's account if the password is forgotten.

Sprint is exploring options for additional security measures to protect its on-line method of access, including changing to a different identifier other than the social security number, while considering the impact on the customer experience and the availability of certain biographical information to data brokers. The recent concerns about access to customer information have involved pretexting rather than hacking into systems as the means of obtaining access to customer information. While Sprint is continuing to research the expense of system changes that would be required to implement various alternatives, we are concerned about devoting potentially significant resources to make changes that may only incrementally improve data security and also will be less customer friendly. Sprint will continue to evaluate CPNI issues and improvement opportunities related to on-line access and will take aggressive action to address any known access breaches.

3. **Online Password Reset:** Sprint's current practices provide the following options: 1) a temporary password is sent to the e-mail address of record; 2) the customer enters the user ID, answers the pre-established security question and is able to reset the password online; or 3) the customer completes an online "contact us" form, including name, billing telephone number and the customer code or the last four digits of the social security number and, upon validation, a new password can be established via e-mail. In addition to the online options, a customer may reset an online password by calling the business office. In that situation, customer identification verification is handled in the same manner as other calls, as set forth in paragraph 1.
4. **Retail Stores:** Sprint does not provide call detail records in retail stores. If a customer were to request the records, the customer would be referred to a local call center. A customer of record may change an account password in a retail store, using the last four digits of the social security number and producing positive photo identification.

Ms. Blanca Bayó

May 5, 2006

Page 3 of 3

5. **Availability of Records:** Sprint considered the option proposed by the Attorney General's office to allow customers to choose to prohibit release of their customer information over the phone or via the internet.

Under this option, customers would essentially be agreeing that they should not be able to access their own information. Sprint believes this option is problematic because there would undoubtedly be situations in which a customer wanted to reverse this decision. An option to reverse the decision presents the same challenges in terms of needing legitimate customer identifiers as are presented by the current access mechanisms discussed above.

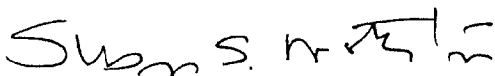
6. **Additional Implementation Measures:** In addition to thoroughly reviewing our processes for improvement opportunities, Sprint is initiating corporate-wide CPNI training that will generally address CPNI regulations and issues, including issues associated with fraudulent access to records. This training will begin in the next month.

Also included with this letter is a copy of the comments Sprint recently filed with the Federal Communications Commission in CC Docket No. 96-115.

Sprint recognizes the vital importance of protecting the privacy of customer account records. Sprint also recognizes that customers expect to be able to access their account information and make changes or ask questions about their service without unreasonable impediments. Sprint believes that its current practices, with the additional security measures discussed above, provide the needed protection without unduly burdening the customer's ability to interact with Sprint. On an ongoing basis, Sprint will continue to evaluate the most effective mechanisms to protect the security of its customers' identities and records.

If you have any questions, or need additional information concerning the attached, please contact me at 599-1560 or Ben Poag at 599-1027.

Sincerely,



Susan S. Masterton

cc: Beth Salak  
Kira Scott  
Rick Moses

**Before the  
Federal Communications Commission  
Washington, DC 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	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277
	)	

**COMMENTS OF SPRINT NEXTEL CORPORATION**

Kent Nakamura  
Heidi Salow  
Sprint Nextel Corporation  
2001 Edmund Halley Drive  
Reston, VA 20191

Douglas G. Bonner  
Kathleen Greenan Ramsey  
Sonnenschein Nath & Rosenthal LLP  
1301 K Street, N.W.  
Suite 600, East Tower  
Washington, D.C. 20005  
(202) 408-6345

Counsel to Sprint Nextel Corporation

Dated April 28, 2006

## SUMMARY

EPIC filed its Petition and the Commission instituted this rulemaking due to the activities of “data brokers.” Such brokers offer to provide the cell phone records of consumers, without the consumer’s permission, to any third party for a fee. Sprint agrees with the Commission that this conduct is disturbing and applauds the Commission’s efforts to combat such conduct. However, the adoption of regulations to address the activities of these data brokers appears to be premature at this time given the actions taken by carriers, state Attorneys General, the Federal Trade Commission, the Federal Communications Commission and Congress.

Moreover, additional regulations directed at carriers are both unnecessary and unworkable. Indeed, Section 222(a) of the Act already imposes an obligation on carriers to protect the proprietary information of customers. In fact, Sprint Nextel has invested significant financial and human resources to protect CPNI on many fronts, including the initiation of state and federal lawsuits against data brokers. Additional regulations are unnecessary because carriers already have obligations to protect CPNI, and they have the ability through technology, internal policies, training and legal action to curtail data broker and “pretexting” activity. With a wide and unique range of internal IT systems, technologies, divisions, affiliates, financial abilities and customer relationships, it is unlikely that any regulation would uniformly solve the problem for all carriers and consumers.

Nonetheless, in the event the Commission finds it necessary to adopt additional regulations, EPIC’s recommendations are not likely to be effective in preventing the activities of data brokers. Sprint Nextel supports solutions that improve data security in a manner that addresses the problem of “pretexting” and that do not compromise the quality of the customer experience. Again, if the Commission feels compelled to adopt additional requirements, Sprint

Nextel urges the Commission to adopt narrowly tailored regulations that recognize the vast differences that exist in network and corporate infrastructures, and avoid the diversion of valuable resources toward ill-conceived solutions that are unlikely to address the problem at hand.

## TABLE OF CONTENTS

I.	ADOPTING NEW REGULATIONS WOULD BE PREMATURE, UNNECESSARY AND UNWORKABLE. ....	2
II.	A RECOGNITION OF THE NATURE AND SCOPE OF THE CPNI PROBLEM MUST UNDERLIE THE ADOPTION OF ANY CPNI DATA SECURITY REGULATIONS. ....	4
III.	SPRINT NEXTEL IS AGGRESSIVELY PROSECUTING LAWSUITS AGAINST ONLINE DATA BROKERS AND FIRMS RESPONSIBLE FOR "PRETEXTING" TO COMBAT THE INVASION OF CUSTOMER PRIVACY BY DATA BROKERS. ....	7
IV.	THE EPIC RECOMMENDATIONS ARE UNDULY BURDENSOME AND WOULD NOT SOLVE THE UNDERLYING PROBLEM. ....	10
A.	Passwords Do Not Eliminate Fraud, But May Help Minimize Fraud. ....	10
B.	Audit Trails Will Not Prevent Unauthorized Disclosure of CPNI. ....	11
C.	Encryption Will Not Prevent Unauthorized Disclosure of CPNI and Is Cost Prohibitive. ....	13
D.	Limiting Data Retention Will Not Prevent Unauthorized Disclosure of CPNI And Cannot Conflict With Various Federal And State Statutory Limitations Periods. ....	15
E.	New Notice Requirements Will Not Prevent Unauthorized Disclosure of CPNI. ....	16
V.	CONCLUSION. ....	17



**Before the  
Federal Communications Commission  
Washington, DC 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	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277
	)	

**COMMENTS OF SPRINT NEXTEL CORPORATION**

Sprint Nextel Corporation ("Sprint Nextel"), through its undersigned counsel, respectfully submits its comments to the Commission's Notice of Proposed Rulemaking ("NPRM") released February 14, 2006 in the above-captioned proceedings.<sup>1</sup> Sprint Nextel applauds the Commission's efforts to ensure the protection of consumer proprietary network information ("CPNI"). Sprint Nextel has a vital interest in ensuring that CPNI is protected from disclosure to unauthorized parties. Sprint Nextel, through its legacy companies,<sup>2</sup> has spent many years, and committed substantial resources, studying and investing in security measures to protect sensitive customer data, including CPNI. To that end, Sprint Nextel has, over time,

---

<sup>1</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Section 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Notice of Proposed Rulemaking (rel. February 14, 2006).

<sup>2</sup> Sprint Corporation and Nextel Communications, Inc. closed the merger of their two companies, including their various operating entities, in August 2005. The integration of the two companies' operations, and merger of various Sprint and Nextel operating affiliates, has also continued since August 2005.

implemented a number of security controls and continues to assess how best to improve its protection of sensitive customer data.

**I. ADOPTING NEW REGULATIONS WOULD BE PREMATURE, UNNECESSARY AND UNWORKABLE.**

In its *NRPM*, the Commission seeks comment on the proposals of the Electronic Privacy Information Center (“EPIC”).<sup>3</sup> EPIC filed its petition and the Commission instituted this rulemaking because of the activities engaged in by so-called “data brokers.” Such brokers claim that they can obtain the “cell phone records” of an individual, including “calls to and/or from a particular cell phone number, the duration of such calls” and perhaps “the physical location of the cell phone.”<sup>4</sup> They also claim that they can “provide calling records for landline and voice over Internet protocol, as well as non-published phone numbers.”<sup>5</sup> Sprint Nextel agrees with the Commission that “this conduct ...[is] very disturbing.”<sup>6</sup> However, although Sprint Nextel shares the security concerns raised by EPIC and the Commission, the adoption of regulations to address the activity of the data brokers appears to be premature at this time given the actions taken by Sprint Nextel<sup>7</sup> and other carriers, state Attorneys General,<sup>8</sup> and by Congress,<sup>9</sup> the Federal Trade Commission,<sup>10</sup> and the Federal Communications Commission.<sup>11</sup>

---

<sup>3</sup> Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) (“EPIC Petition”).

<sup>4</sup> *NRPM* at ¶ 1.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.* For this reason among others, Sprint has filed a number of lawsuits against data brokers. *See infra* n.14.

<sup>7</sup> *See infra* at n.14.

Moreover, imposing new regulations on carriers would be unnecessary and unworkable. Indeed, Section 222(a) of the Act already imposes an obligation on carriers to protect the proprietary information of customers. In fact, Sprint Nextel has invested significant financial and human resources to protect CPNI, such as the substantial resources necessary to pursue legal action against data brokers. Additional regulations are unnecessary because carriers already have a duty to protect CPNI, and carriers have the ability through technology, internal processes and policies, training of customer service personnel, and legal action to curtail unlawful data broker and "pretexting" activity. Furthermore, new carrier regulations would be unworkable given the array of carrier networks, technologies, divisions, affiliates, financial abilities and

---

<sup>8</sup> Madigan Sues Second Company That Sells Cell Phone Records, Illinois Attorney General Press Release at [http://www.ag.state.il.us/pressroom/2006\\_03/20060315c.html](http://www.ag.state.il.us/pressroom/2006_03/20060315c.html); *see also*, Locatecell.com must stop selling cell phone records of Missourians, under court order obtained by Nixon, Missouri Attorney General's Office, Press Release at <http://www.ago.mo.gov/newsrelease/2006/021506.htm>; *see also*, Florida Sues Data Broker Over Sale of Phone Records at [http://www.consumeraffairs.com/news04/2006/02/fl\\_global.html](http://www.consumeraffairs.com/news04/2006/02/fl_global.html).

<sup>9</sup> *See, e.g.*, Washington Internet Daily, April 27, 2006, at 9 (on April 25, 2006 the House unanimously passed the cellphone privacy bill (HR-4709) that was voted out of the Judiciary Committee March 2, 2006); Washington Internet Daily, Apr. 7, 2006, at 9-10 (House Commerce Committee subpoenaed twelve data broker companies that offer to sell detailed records of private phone calls); Data-Breach Disclosure Bill Passes House Panel, Roy Mark, internetnews.com, Mar. 30, 2006, available at [www.internetnews.com/bus-news/article.php/3595291](http://www.internetnews.com/bus-news/article.php/3595291) ("Legislation forcing data brokers to disclose security breaches to the public passed the U.S. House Energy and Commerce Committee [on March 30, 2006] on a 41-0 vote).

<sup>10</sup> Prepared Statement of The Federal Trade Commission before the Committee on Energy and Commerce, U.S. House of Representatives (February 1, 2006); *see also*, Prepared Statement of The Federal Trade Commission before the Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Affairs, Product Safety, and Insurance, U.S. Senate (February 8, 2006).

<sup>11</sup> Citation issued by Letter to Steven Schwartz, LocateCell.com, from Colleen Heitkamp, Federal Communications Commission, DA 06-124 (January 20, 2006); Citation issued by Letter to James Kester, DataFind.org, from Colleen Heitkamp, Federal Communications Commission, DA 06-122 (January 20, 2006).

customer relationships, it is unlikely that any regulation would uniformly solve the problem for all carriers and consumers.

Nonetheless, should the Commission feel compelled to adopt additional regulations, Sprint Nextel does not believe that any of EPIC's proposed changes are likely to be effective in preventing the types of unauthorized disclosures of CPNI that gave rise to the EPIC Petition. Sprint Nextel supports solutions that improve data security in a manner that addresses the problem of "pretexting" without compromising the quality of the customer experience. If, after reviewing the entire record, the Commission concludes that it must adopt new regulations, Sprint Nextel urges it to adopt narrowly tailored regulations that recognize the wide differences that exist in network and corporate infrastructures, and avoid the diversion of valuable resources toward ill-conceived solutions that are unlikely to address the problem at hand.

**II. A RECOGNITION OF THE NATURE AND SCOPE OF THE CPNI PROBLEM MUST UNDERLIE THE ADOPTION OF ANY CPNI DATA SECURITY REGULATIONS.**

In order to respond appropriately to the issues in the *NPRM*, it is critical as a threshold matter to define the nature and scope of the problem. As the EPIC Petition makes clear, the major threat to customer privacy is the acquisition of CPNI by unauthorized persons such as data brokers. Based on Sprint Nextel's experience, attempts to gain unauthorized access to CPNI typically involve (1) "pretexting" or social engineering tactics used by certain persons (*i.e.*, data brokers, private investigators, or personal acquaintances of the customer) in possession of sufficient personal information about the customer to pose as the customer, (2) repeated non-technical "probes" to identify and exploit vulnerabilities in the organization's identity

verification processes,<sup>12</sup> and (3) the use of voice distortion devices or TTY equipment by individuals pretending to be speech or hearing impaired.

The Commission asks whether data brokers are able to obtain customers' proprietary information "through 'hacking' or otherwise obtaining unauthorized access to consumers' online accounts with communications carriers."<sup>13</sup> At least in Sprint's Nextel's experience, the answer is no. Sprint Nextel is unaware of any instance in which an unauthorized person obtained CPNI by electronically "hacking" into any Sprint Nextel information system. This is not surprising, given Sprint Nextel's robust information security infrastructure. Accordingly, any proposals to address the problem at hand should specifically target the vulnerabilities outlined above which, based on Sprint Nextel's experience, give rise to the problem.

If the Commission does not focus on the source of the problem, Sprint Nextel is concerned that a complex array of costly, overly burdensome and ineffective new rules may result. This will force carriers to devote considerable resources to comply with new rules, while losing focus on the overall goal of protecting CPNI from unauthorized disclosure. Worse, overreaching new rules could have the harmful unintended consequence of impairing the efficient service that Sprint Nextel customers have come to expect. Any new rules should provide flexibility to allow carriers to protect CPNI given a host of issues that carriers face,

---

<sup>12</sup> For example, a data broker may call a carrier's call center repeatedly in an attempt to garner some piece of information about a customer or the customer's account. If successful in obtaining one piece of information about a customer or the account, the data broker may continue calling, each time learning one more piece of information. Ultimately, the data broker may use this information, together with the other information from publicly available sources, to convince the agent to reset a "forgotten" password. The new password could then be used to obtain online access to the customer's account records.

<sup>13</sup> *NPRM* at ¶11.

including tailoring security level requirements based upon specific customer demand (e.g., a law enforcement customer may demand a level of protection beyond that desired by an individual consumer). In fact, "one size fits all" solutions are unlikely to prove workable for an industry in which the nature of the carrier-customer relationship differs dramatically depending on the type of service at issue, and where carriers have multiple internal systems and procedures supported by differing technology. Furthermore, any such rules must take into account the fact that a series of recent mergers and acquisitions have forced carriers like Sprint Nextel to devote significant resources to integrating preexisting security measures and systems.<sup>14</sup>

In addition to the concerns raised above, Sprint Nextel believes that the Commission should take into account the considerable enforcement mechanisms that presently exist to

---

<sup>14</sup> The Sprint Nextel merger, consummated on August 12, 2005, was approved by the Commission on August 8, 2005. *In the Matter of Applications of Nextel Communications, Inc. and Sprint Corporation for Consent to Transfer Control of Licenses and Authorizations*, FCC WT Docket No. 05-63 Memorandum Opinion and Order (rel. August 8, 2005), see [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-05-148A1.doc](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-148A1.doc). As of September 30, 2005, according to SEC filings, the total subscriber base served by Sprint Nextel including its wireless affiliates, resellers of Sprint Nextel's wireless service, and its incumbent local exchange subsidiaries, was 54.9 million subscribers. This major merger, creating the third largest wireless carrier in the U.S., is still less than one year old, and Sprint Nextel is continuing to implement its post-merger reorganization.

Other mergers and acquisitions have occurred as a consequence of the Sprint Nextel merger, including the acquisitions of the following Sprint PCS affiliates: IWO Holdings, Inc., Gulf Coast Wireless, Enterprise Communications Partnership, Alamosa Holdings (the largest Sprint PCS wireless affiliate with approximately 1.5 million direct wireless subscribers) and UbiquiTel, Inc. News Releases: "Sprint Nextel to Acquire Wireless Affiliate UbiquiTel Inc." (April 20, 2006), at [http://www2.sprint.com/mr/news\\_dtl.do?id=11440](http://www2.sprint.com/mr/news_dtl.do?id=11440); "Sprint Nextel Completes Acquisition of Wireless Affiliate Alamosa Holdings" (Feb. 1, 2006), at [http://www2.sprint.com/mr/news\\_dtl.do?id=10040](http://www2.sprint.com/mr/news_dtl.do?id=10040); "Sprint Nextel to Acquire Wireless Affiliate Enterprise Communications Partnership" (Dec. 16, 2005), at [http://www2.sprint.com/mr/news\\_dtl.do?id=9520](http://www2.sprint.com/mr/news_dtl.do?id=9520); "Sprint Nextel Completes Acquisition of IWO Holdings, Inc." (Oct. 20, 2005), at [http://www2.sprint.com/mr/news\\_dtl.do?id=8740](http://www2.sprint.com/mr/news_dtl.do?id=8740); "Sprint Nextel Completes Wireless Affiliate Transaction" (Oct. 3, 2005), at [http://www2.sprint.com/mr/news\\_dtl.do?id=8600](http://www2.sprint.com/mr/news_dtl.do?id=8600).

Finally, a put price was determined for the purchase by Sprint Nextel of the shares of Nextel Partners in late December, 2005.

address these concerns, and the decisive action already being taken by carriers, including Sprint Nextel, to combat these issues. First, the Commission already has the power to sanction carriers who insufficiently protect CPNI.<sup>15</sup> Second, the market is self-regulating, as customers concerned about security will naturally migrate to those carriers who offer the best perceived security practices, particularly in light of the publicity surrounding CPNI breaches over the past year. Finally, a number of carriers, including Sprint Nextel, have taken aggressive action against data brokers by filing lawsuits against the data brokers who have advertised the sale of customer phone records.<sup>16</sup> Indeed, the most well-known data brokers have had their CPNI sales shut down as a result of carrier lawsuits, and have been sued or investigated by state Attorneys General, the Federal Trade Commission and the Federal Communications Commission.<sup>17</sup>

**III. SPRINT NEXTEL IS AGGRESSIVELY PROSECUTING LAWSUITS AGAINST ONLINE DATA BROKERS AND FIRMS RESPONSIBLE FOR “PRETEXTING” TO COMBAT THE INVASION OF CUSTOMER PRIVACY BY DATA BROKERS.**

Sprint Nextel has been among the most aggressive telecommunications carriers in the country in filing lawsuits against online data brokers and entities engaging in “pretexting” to obtain unauthorized access to customer call records. For some time, Sprint Nextel has had a full

---

<sup>15</sup> Section 503(b) of the Communications Act authorizes the Commission to assess a forfeiture of up to \$130,000 for each violation of the Act or of any rule, regulation, or order issued by the Commission under the Act. The Commission may assess this penalty if it determines that the carrier’s noncompliance is “willful or repeated.” On January 30, 2006, the Commission issued Notices of Apparent Liability (“NAL”) for Forfeiture in the amount of \$100,000 each against two telecommunications carriers for violating 47 C.F.R. § 64.2009(e) of the Commission’s rules.

<sup>16</sup> *Sprint Nextel Corp. d/b/a Sprint Nextel v. 1<sup>st</sup> Source Information Specialists, Inc., et al.*, Broward County, Florida Circuit Court Case No. 06001083 (02) (filed Jan. 26, 2006); *Sprint Nextel Corp. d/b/a Sprint Nextel v. All Star Investigations, Inc., et al.*, Miami-Dade County, Florida Circuit Court Case No. 06 01736 (filed Jan. 27, 2006); *Sprint Nextel Corp. d/b/a Sprint Nextel v. San Marco & Associates Private Investigation, Inc., et al.*, Case No. 8:06-CV-00484-T-17TGW (MD. Fla.) (filed March 17, 2006).

<sup>17</sup> See *supra* n.5-9.

scale investigation underway of entities that access or attempt to access Sprint Nextel customer data without permission.<sup>18</sup> In addition to lawsuits filed by other leading wireless carriers in the past six (6) months, Sprint Nextel has filed three (3) lawsuits this year alone to help minimize this threat. Some of the most well-known data brokers have had their CPNI sales shut down as a result of carrier lawsuits. For example, as a result of Sprint Nextel's lawsuit filed against an online data broker in January, 2006, Sprint Nextel has secured a permanent injunction against the parent company of several online data brokers, and the Company's principals, preventing them from attempting to obtain, sell or distribute call detail records of Sprint Nextel customers.<sup>19</sup> Even those targeted defendants who have not yet formally agreed to, or been the subject of, a court-ordered injunction precluding the continued procurement or sale of customer call records appear to have curtailed such fraudulent activities after they have been sued. It is clear that these carrier lawsuits against online data brokers and firms that engage in pretexting has had a chilling effect on those that engage in these pretexting activities for profit. Sprint Nextel has publicly committed to taking further action that may be necessary, including further lawsuits, to eliminate this threat.<sup>20</sup>

Notwithstanding these successful litigation results over the past several months as a result of litigation by Sprint Nextel and other carriers, Sprint Nextel recognizes that the Commission and carriers have roles to bolster the protection of CPNI. First, Sprint Nextel believes strongly

---

<sup>18</sup> See, News Release, "Sprint Nextel Files New Lawsuit to Halt Fraudulent Pursuit of Confidential Customer Information" at [http://www2.sprint.com/mr/news\\_dtl.do?id=9960](http://www2.sprint.com/mr/news_dtl.do?id=9960).

<sup>19</sup> See, News Release, "Sprint Nextel Files Lawsuit Against Fraud Source in Ongoing Effort to Protect Consumer Privacy," (March 20, 2006) at [http://www2.sprint.com/mr/news\\_dtl.do?id=10920](http://www2.sprint.com/mr/news_dtl.do?id=10920)

<sup>20</sup> *Id.*



that increasing consumer awareness about the steps consumers can take to protect their own information is essential,<sup>21</sup> and would support the Commission's leadership on a consumer education outreach initiative. Sprint Nextel strongly encourages its customers to take precautions to protect themselves, to include changing passwords used to access account information. It also provides customers access to privacy tips on its website.<sup>22</sup> Second, Sprint Nextel notes that carriers have an ongoing legal and business obligation to train new and existing employees, to review internal policies and procedures, and to address employee misconduct related to the unauthorized release of CPNI. Given the recent Commission enforcement activities, carriers are reminded of their obligations and will inevitably increase their efforts to protect CPNI. Accordingly, Sprint does not believe there is a genuine need for new rules at this time.

However, if the Commission decides otherwise, Sprint Nextel emphasizes that any new rules must allow for implementation of security controls on a technology-neutral basis, and allow carriers discretion based on the differences in their internal systems. Carriers should be granted the flexibility to select the security policies, processes, and technology controls that will most efficiently and effectively protect CPNI within their existing information systems, without

---

<sup>21</sup> See e.g., "Headlines: Sprint Nextel's Commitment to Customer Privacy," at [http://www2.sprint.com/mr/cda\\_pkDetail.do?id=1100](http://www2.sprint.com/mr/cda_pkDetail.do?id=1100). This Web page, one of the most frequently visited on the Sprint Web site, raises awareness of these issues amongst consumers, and provides tips as to how to help combat this problem.

<sup>22</sup> See, e.g., News Release, "Sprint Nextel Files New Lawsuit to Halt Fraudulent Pursuit of Confidential Customer Information" (January 30, 2006) at [http://www2.sprint.com/mr/news\\_dtl.do?id=9960](http://www2.sprint.com/mr/news_dtl.do?id=9960); News Release, "Sprint Nextel Files Lawsuit Against Fraud Source in Ongoing Effort to Protect Consumer Privacy," (March 20, 2006) at [http://www2.sprint.com/mr/news\\_dtl.do?id=10920](http://www2.sprint.com/mr/news_dtl.do?id=10920).

requiring wholesale retrofitting of existing systems. The ultimate goal should be the protection of CPNI from unauthorized disclosure.

**IV. THE EPIC RECOMMENDATIONS ARE UNDULY BURDENSOME AND WOULD NOT SOLVE THE UNDERLYING PROBLEM.**

Sprint Nextel has evaluated the rules proposed by EPIC.<sup>23</sup> Several of the recommendations place unnecessary burdens on carriers without meaningfully contributing to the overall goal of protecting CPNI from unauthorized disclosure. Sprint Nextel's remarks regarding each of the specific proposals are set forth below.

**A. Passwords Do Not Eliminate Fraud, But May Help Minimize Fraud.**

In its Petition, EPIC proposes that the Commission require carriers to implement consumer-set passwords to protect the security of CPNI. EPIC states that data brokers collect consumer biographical data (*e.g.*, date of birth, mother's maiden name, etc.) that carriers often use to authenticate the identity of customers, thereby allowing the brokers to obtain unauthorized access to CPNI.<sup>24</sup> Sprint Nextel believes that passwords can be an effective method for protecting CPNI,<sup>25</sup> but the Commission and the public must be mindful of their limitations. For example, consumer set passwords will prove no bar to an ex-spouse, family member or significant other from exploiting their knowledge of a password to secure customer data. Likewise, an inherent difficulty in mandating that consumers select passwords is establishing a

---

<sup>23</sup> In its *NPRM*, the Commission requests comment on the issues raised by EPIC. *NPRM* at ¶ 9. Therefore, Sprint Nextel comments on the specific proposals set forth by EPIC.

<sup>24</sup> EPIC Petition at 8.

<sup>25</sup> To the best of Sprint Nextel's knowledge, most wireless carriers already require the use of a password for account access via the Web, and many require passwords for other methods of account access as well. These password regimes are presumably created in a manner that considers the needs of the customer, most important the customer's need for timely and efficient handling of inquiries.

“fraud-proof” password reset process for forgotten passwords. Inevitably, a certain percentage of customers forget their passwords once, or even more often, when attempting to access their accounts. When this happens, carriers need to ask personal questions that allow the customer to establish his or her identity before the password can be reset. This authentication process lends itself to the pretexting problem, since fraudsters can easily access personally identifiable information about consumers. In addition, independent research indicates that consumers find mandatory passwords to be inconvenient.<sup>26</sup> Thus, Sprint Nextel urges that the Commission be wary of adopting a rule mandating that consumers submit a password for access to all account information, regardless of the means by which a customer attempts to access such information, when such rule will not prevent all unauthorized access to CPNI.

If the Commission decides otherwise, it must balance such a mandate against consumers’ requests for convenient access to their account data. Sprint Nextel suggests a rule requiring carriers to make a customer-set password feature widely available to consumers who choose added protection for their accounts - but without mandating the use of passwords for all types of account access.<sup>27</sup>

**B. Audit Trails Will Not Prevent Unauthorized Disclosure of CPNI.**

In its Petition, EPIC recommends that carriers record all instances of access to a customer record.<sup>28</sup> Sprint Nextel generally supports the use of audit trails as a means of facilitating

---

<sup>26</sup> “The Ponemon Report: Those Pesky Passwords,” Larry Ponemon, *available at* [www.csoonline.com/read/030106/ponemon](http://www.csoonline.com/read/030106/ponemon) (“Too many and too complicated to remember, passwords make users crazy and incur help desk expense. What should you do about it?”).

<sup>27</sup> It is worth noting that there are many methods for verifying a customer’s identity. For example, a carrier may require a customer’s driver’s license, social security number, recent phone bill or other information personal to a customer.

<sup>28</sup> EPIC Petition at 11.

internal investigations into how fraudulent activity may have taken place, and disciplining rogue employees who improperly release CPNI. Sprint Nextel's customer service procedures already address the handling of potentially "suspicious" situations or fraudulent activity, and these procedures were well established even before third party "pretexters" came out of the woodwork. It is also important to acknowledge that audit trails, while possibly helpful in the eventual attribution of responsibility for the improper release of CPNI, will not prevent the unauthorized release of CPNI. For example, an audit trail system that tracks each and every question asked by a customer service representative during the course of an inbound call would not solve the social engineering problem. If a pretexter knows the answers to the questions, the audit trail indicates only that correct answers were provided. Further, the costs involved in implementing extensive audit trails across different systems are considerable, and could substantially outweigh any benefits of implementation. The Commission has previously acknowledged that requiring carriers to implement audit trails that would keep track of all access to CPNI would place too great a burden on carriers:

... the *CPNI Order's* electronic audit trail requirement would generate "massive" data storage requirements at great cost. As it is already incumbent upon all carriers to ensure that CPNI is not misused and that our rules requiring the use of CPNI are not violated, we conclude that, on balance, such a potentially costly and burdensome rule does not justify its benefit.<sup>29</sup>

These burdens are further complicated by the fact that the technical requirements of implementing audit trails vary widely among various operating systems and applications. Sprint Nextel currently has an extremely large number of different systems housing billing and

---

<sup>29</sup> *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 171 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, para. 127 (1999).

customer account information after its recent August 2005 merger and subsequent mergers with legacy company affiliates.

Finally, it should be noted that the Commission's CPNI rules already require carriers to maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI,<sup>30</sup> and that carriers have a means to audit their procedures so that they can submit the annual CPNI certification.<sup>31</sup>

For the reasons explained above, Sprint Nextel recommends against any new rules requiring inflexible and exhaustive audit trail functionality. At the very least, any rules the Commission decides to implement concerning audit trails should be flexible and technology-neutral, allowing carriers to implement audit solutions that are feasible for their current technology infrastructures. Finally, any new rule should be narrowly tailored to achieve the objective of unearthing actual instances of unauthorized release of CPNI, and not merely require carriers to log meaningless data.

**C. Encryption Will Not Prevent Unauthorized Disclosure of CPNI and Is Cost Prohibitive.**

In its Petition, EPIC recommends that the Commission implement rules requiring all CPNI data stored by carriers to be encrypted.<sup>32</sup> Like so many of the EPIC recommendations, it is very unlikely that encryption of stored CPNI would have prevented the incidents that gave rise to the Commission's Rulemaking. Data brokers (and other unauthorized parties) obtained access to CPNI through the use of "pretexting" and by exploiting vulnerabilities in front-end

---

<sup>30</sup> See 47 C.F.R. § 64.2009 (c).

<sup>31</sup> See 47 C.F.R. § 64.2009 (e).

<sup>32</sup> EPIC Petition at 11.

authentication protocols administered both by employees and automated systems. Sprint Nextel is unaware of any instances of data brokers gaining unfettered access to electronic customer databases. In other words, even if carriers had encrypted all CPNI data stored in databases, data brokers would still have gained access to CPNI at the very points at which it was converted to plain text -- when a purportedly authorized person (either the customer or an employee) requested it. Accordingly, encryption may prevent third parties from gaining access to CPNI through sophisticated computer hacking attempts, but it would be useless in thwarting pretexting attempts which are at the heart of the petition.

By contrast, Sprint Nextel has implemented a host of other IT security measures that do provide meaningful safeguards to protect CPNI. For example, Sprint Nextel has implemented firewalls at all points of entry into its network. It has also deployed intrusion detection systems (IDS) at all Internet points of entry. Sprint Nextel has also implemented company-wide procedures requiring management approval for the on-boarding or off-boarding of users, implemented fraud alert and incident response procedures, and required security awareness training for its employees. It has a single, centralized security department responsible for the oversight of security policy, awareness, and enforcement throughout the company. Finally, Sprint Nextel continuously reassesses its processes for the security of customer data.

Given that encryption of customer records, while housed in carriers' databases, is unlikely to provide any real protection against existing threats to CPNI, Sprint Nextel strongly opposes any rules requiring its use. Sprint Nextel has a wide array of divergent information systems that have not yet been integrated after the company's recent merger. Enterprise encryption solutions are extremely expensive and can be difficult to implement across different

platforms and systems. Forcing carriers to invest the extensive resources necessary to implement encryption would divert necessary financial and personnel resources away from security measures that are effective in preventing data brokers and other unauthorized parties from obtaining access to CPNI.

**D. Limiting Data Retention Will Not Prevent Unauthorized Disclosure of CPNI And Cannot Conflict With Various Federal And State Statutory Limitations Periods**

EPIC suggests that carriers should be required to delete customer call records when they are no longer needed for billing purposes or to settle disputes.<sup>33</sup> Sprint Nextel's data storage policies are dictated by a number of factors including, but not limited to, the need to resolve billing disputes, the needs of law enforcement, the needs of state tax auditors, and for litigation purposes. Sprint Nextel's data retention policies take into account variations in applicable federal and state statutes of limitation for contesting contract provisions. Storage of data for periods longer than necessary for business purposes or compliance with applicable laws is a costly practice that, in this competitive environment, no carrier has an incentive to indulge. Sprint Nextel believes that additional rules of this nature are unnecessary, but at a minimum, any rules requiring the deletion of customer call records must account for the necessary statutory limitation periods.

---

<sup>33</sup> EPIC Petition at 11.

**E. New Notice Requirements Will Not Prevent Unauthorized Disclosure of CPNI.**

In its Petition, EPIC recommends implementing rules requiring carriers to notify customers when their CPNI may have been breached.<sup>34</sup> Sprint Nextel opposes the implementation of any such rule because it would not achieve the ultimate goal of this NPRM, which is to prevent the disclosure of CPNI to unauthorized parties. Additionally, a majority of states have their own data breach notification laws in place requiring any business to notify customers when they suffer a data breach that compromises the security of sensitive personal information. These data breach laws are designed to ensure that consumers know when their data has been breached so they can take the proper steps to prevent identity theft. Most carriers, including Sprint Nextel, have invested in policies and practices to ensure that they comply with these state laws in the event a breach occurs. Creating an additional notice regime for CPNI breaches would be extremely expensive and, as stated previously, would not accomplish the main goal of preventing the disclosure of CPNI to unauthorized parties. Much like encryption, requiring such expansive notice would be a solution ill-suited to solving the problem at hand.

Moreover, Sprint Nextel's experience has shown that customers are generally the first to learn that their information has been wrongfully acquired or misused, not the carrier. If a customer inquires as to whether his/her information has been accessed or released, the carrier would, as a best practice, conduct an internal investigation. In some cases, the investigation may not conclusively determine that a customer's account was in fact accessed without the customer's authorization.

---

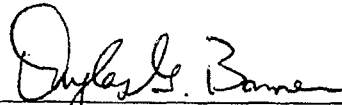
<sup>34</sup> *Id.*



**V. CONCLUSION**

The protection of CPNI is a serious issue, and is one in which the telecommunications industry already has strong incentives to self-police. As discussed herein, Sprint Nextel believes that the telecommunications industry, in combination with the interested government agencies, is taking proactive steps to address the threat of data brokers and "pretexting" to obtain customer data. Given the complexity and variation of billing systems, front-end software and authentication processes amongst carriers, it is best to allow carriers maximum flexibility in determining the best way to protect against unauthorized access to CPNI.

Respectfully submitted,



---

Douglas G. Bonner  
Kathleen Greenan Ramsey  
Sonnenschein Nath & Rosenthal LLP  
1301 K Street, N.W.  
Suite 600, East Tower  
Washington, D.C. 20005  
(202) 408-6400

Counsel for Sprint Nextel Corporation

Kent Nakamura  
Heidi Salow  
Sprint Nextel Corporation  
2001 Edmund Halley Drive  
Reston, VA 20191

Dated April 28, 2006