

**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 VERIZON WIRELESS**

John T. Scott, III  
Charon H. Phillips  
1300 I Street, N.W.  
Suite 400 West  
Washington, D.C. 20005  
(202) 589-3740

April 28, 2006

Its Attorneys

**TABLE OF CONTENTS**

**SUMMARY .....ii**

**I. ADDING MORE CPNI PROCEDURES WILL NOT STOP PRETEXTING, WHICH IS DESIGNED TO EVADE THOSE PROCEDURES.....2**

**II. CARRIERS ALREADY HAVE THE DUTY AND THE INCENTIVE TO PROTECT THEIR CUSTOMERS’ PRIVATE INFORMATION.....3**

**III. THE FCC SHOULD REJECT MANY OF THE PROPOSALS IN THE NOTICE BECAUSE THEY WILL NOT STOP PRETEXTERS.....7**

**A. Mandatory Passcodes Would Burden Customers and Can Themselves Be Socially Engineered .....8**

**B. The FCC Should Not Adopt an Opt-in Requirement for Disclosure of CPNI to Joint Venture Partners and Independent Contractors .....9**

**C. Audit Trails Would Have Little Value Against Pretexting.....12**

**D. Encryption Requirements Would Not Deter Social Engineering.....15**

**E. The FCC Should Not Require Customer Notification .....15**

**F. Limiting Data Retention Would Not Impact Social Engineering and is Not Consistent With Certain Mandated Retention Requirements .....17**

**IV. VERIZON WIRELESS SUPPORTS TWO NEW RULES AND A SET OF PRACTICES THAT WOULD DEFINE A SAFE HARBOR FROM ENFORCEMENT .....18**

**A. Carriers Should Post Their Privacy Policies and File Their CPNI Certifications With the Commission .....18**

**B. The Commission Should Adopt a Set of Procedures That If Implemented Would Serve as a Safe Harbor From FCC Enforcement .....20**

**CONCLUSION .....22**

## SUMMARY

The best way to stop pretexters is to put them out of business. Individuals and entities that fraudulently obtain call records and other proprietary customer information should be met with aggressive law enforcement and litigation. Verizon Wireless has led the industry in efforts to find these con artists and enjoin their activities. In contrast, imposing additional “CPNI” rules on carriers is not an effective way to address the problem. The Commission should reject most of the proposals in the *Notice* because they aim in the wrong direction, by adding costs and burdens on carrier and their customers without effectively stopping pretexting. Audit trails, encryption, opt-in consent, and similar mandates would not discourage pretexting. Rigid new FCC rules that standardize industry practices could in fact be counterproductive by providing pretexters with a roadmap to chart new forms of social engineering.

Instead, the Commission should continue its efforts in conjunction with the Federal Trade Commission and law enforcement agencies to crack down on the wrongdoers. It should adopt two new requirements for carriers to provide customers and the Commission with updated information on privacy safeguards. It should also adopt a set of best practices procedures that when implemented by a carrier would constitute a “safe harbor” from enforcement, for the same reasons that it adopted a safe harbor for inadvertent violations of its Do-Not-Call rules. Carriers who seek in good faith to protect their customers’ privacy by adopting and following procedures to train and alert their employees should not be penalized by the deceptive conduct of third parties.

**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 VERIZON WIRELESS**

Verizon Wireless respectfully submits these comments on the *Notice*<sup>1</sup> responding to the *Petition*<sup>2</sup> filed by the Electronic Privacy Information Center (“EPIC”). The Commission should not require carriers to standardize their procedures or adopt costly new practices that would not provide meaningful protection against social engineers. Instead, the Commission should adopt limited new rules, and follow the same approach it used in the Do-Not-Call proceeding of identifying “safe harbor” safeguards that can be implemented by carriers.

---

<sup>1</sup> Implementation of the Telecommunications Act of 1996; 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, *Notice of Proposed Rulemaking*, FCC No. 06-10 (rel. Feb. 14, 2006).

<sup>2</sup> Petition of the Electronic Privacy Information Center For Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, filed August 30, 2005 (“*Petition*”).

**I. ADDING MORE CPNI PROCEDURES WILL NOT STOP PRETEXTING, WHICH IS DESIGNED TO EVADE THOSE PROCEDURES.**

While the problem of pretexting should not be minimized, the combined efforts of the FCC, the Federal Trade Commission, law enforcement officials, and carriers such as Verizon Wireless have put many pretexters out of business.<sup>3</sup> Although the *EPIC Petition* and the *Notice* appropriately discuss the importance of safeguarding CPNI, there is a real question as to whether the proposals offered by EPIC and the *Notice* would have any impact on pretexting.

Before adopting any new rule, the Commission must determine whether it will in fact thwart or stop pretexters. All carriers already have the duty under existing rules and the Communications Act to protect their customers' CPNI. Adding rigid requirements for how they must discharge that duty risks standardizing carrier practices in ways that may enable pretexters to exploit those practices. Worse, such requirements may prove counterproductive by disincenting carriers from experimenting with new practices to protect CPNI. For example, a rule that carriers retain "audit trails" of how CPNI was used would impose massive record retention obligations on carriers, who may use CPNI literally millions of times each month to educate their customers on new products and services and respond to customers' inquiries. But it is unclear how such a rule would impede pretexting, which succeeds by fraudulently inducing a carrier employee to disclose a customer's proprietary information in the belief that the employee is assisting that customer. The employee may diligently comply with the audit trail rule by creating

---

<sup>3</sup> Verizon Wireless continues to urge the FCC to coordinate with the Department of Justice and Federal Trade Commission pursuant to its broad authority under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and to develop a joint enforcement task force to address these matters.

an electronic or other record of the CPNI “use,” but the CPNI is already in the hands of the pretexter. Put another way, even if all carriers had been under the type of audit tracking mandates that EPIC suggests a year ago, there is no basis to conclude that such a mandate would have discouraged any of the pretexters whose conduct has been exposed through the work of carriers and law enforcement agencies over the past months.

In essence, the problem that motivated EPIC’s petition and the *Notice* is not a carrier “CPNI practice” problem that warrants imposing the proposed new regulations on carriers. Rather the problem is that a limited number of individuals and entities have found a market for selling customer information, providing them the incentive for fraudulently obtaining that information. The solution is to ensure there are laws aimed at the unlawful conduct itself, and to devote government resources to enforcing those laws to put pretexters out of business.

## **II. CARRIERS ALREADY HAVE THE DUTY AND THE INCENTIVE TO PROTECT THEIR CUSTOMERS’ PRIVATE INFORMATION.**

Carriers also already have ample incentive to impose their own safeguards to protect CPNI because the failure to do so will cost them customers. No carrier wants to receive a call or letter from an irate customer complaining about the disclosure of his or her call detail information to an estranged spouse or other person. Verizon Wireless’s efforts underscore these points. As detailed in its initial comments on the *Petition*, Verizon Wireless takes its customers’ privacy very seriously. Verizon Wireless has always maintained internal safeguards and procedures for the use and disclosure of CPNI and reviews those safeguards continually to determine whether modifications should be made. In response to the emerging threat from social engineers, Verizon Wireless has

focused on adopting procedures that are designed to stop this deceitful activity in the manner it typically occurs.

In most documented cases, data brokers have obtained CPNI through multiple fraudulent and deceptive phone calls to customer service. Verizon Wireless is not aware of any cases in which data brokers were able to obtain such information through “hacking” into Verizon Wireless systems or through a Verizon Wireless employee. More typically, pretexters may pose as Verizon Wireless employees and even provide customer service representatives with valid employee names and identification numbers. Customer service representatives are thus on the front line in the fight against this problem. Social engineers seek to capitalize on the fact that in the competitive wireless industry, carriers must distinguish themselves with respect to customer service to retain customers.

Given that calls to customer service are pretexters’ main source of information, it is essential to educate customer service representatives to recognize social engineering and the particular methods that social engineers employ in these scams. To this end, Verizon Wireless has had an extensive training program that fully informs all employees, including sales and marketing personnel, about the CPNI rules and the specifics of social engineering techniques, and that disregard of CPNI rules can be the grounds for disciplinary action. Verizon Wireless maintains a comprehensive Code of Business Conduct, trains new employees at time of hire on the Code and offers generalized and specialized training on the Code throughout the year. The Code defines CPNI and specifically prohibits its disclosure unless the information must be produced pursuant to subpoena or other valid legal process. New hires are provided with a copy of the Code along with their offer letter.

Verizon Wireless's Office of Integrity and Compliance ("OIC") has primary responsibility for drafting, disseminating and training on the Code. It also maintains a confidential 800 number for employees to report possible violations of the Code, including violations related to customer privacy. Employees are advised of the 800-number via the Code, postings in the workplace, periodic e-mails, and an OIC brochure. The OIC brochure specifically instructs employees to report "misuse of confidential or proprietary information." Training on maintaining security of CPNI includes:

- Initial code and web-based training on privacy for all employees.
- E-mail alerts to all employees.
- Postings on the Verizon Wireless internal intranet site, "VZ Web."
- Quarterly distribution to all employees of "Integrity Times," a newsletter addressing ethics/compliance issues, including protection of CPNI and guarding against pretexting.
- Written Methods & Procedures for customer care representatives and marketing personnel, detailing required procedures for identifying and verifying subscribers and protecting CPNI.

Verizon Wireless's Workforce Development and Training Group is responsible for new hires and all developmental training for Verizon Wireless employees. Verizon Wireless requires employees to take numerous specific courses that address the need to protect the privacy of customer information, and instructs employees, through written materials and classroom exercises, on procedures for doing so.

In addition to these internal measures, Verizon Wireless was the first private or public entity to investigate incidents of "pretexting," and it was the first to file lawsuits against individuals and companies who attempted to obtain customer information through fraudulent means. Verizon Wireless has won injunctions to stop those practices. For example, on September 15, 2005, Verizon Wireless obtained a permanent injunction

against Source Resources, Inc., a Tennessee company that advertised on its web site that it could obtain wireless telephone records and other confidential customer information.<sup>4</sup>

On November 9, 2005, Verizon Wireless obtained a temporary restraining order against Global Information Group (GIG), a Florida company which had made thousands of attempts to gather confidential information without proper authorization and used various fraudulent schemes to do so, including impersonating Verizon Wireless employees and posing as Verizon Wireless customers.<sup>5</sup>

On January 30, 2006, Verizon Wireless won a preliminary injunction against Data Find Solutions, First Source Information Specialists, and related companies in U.S. District Court in Trenton, New Jersey.<sup>6</sup> These companies are the current and former owners of the websites locatecell.com, celltolls.com, peoplesearchamerica.com, and datafind.org. The lawsuit alleged that these companies fraudulently attempted to obtain customer records by calling Verizon Wireless customer service centers posing as Verizon Wireless employees needing access to confidential customer information. The injunction prohibits these data brokers from attempting to obtain information on Verizon Wireless customers, providing any information on Verizon Wireless customers to any third parties, or operating any website that may advertise that they can obtain information on Verizon Wireless customers.

---

<sup>4</sup> *Cellco Partnership d/b/a Verizon Wireless v. Source Resources*, Permanent Injunction on Consent, Docket No. SOM-L-1013-05 (Sup. Ct. of N.J.; Law Div.: Somerset County, Sept. 13, 2005).

<sup>5</sup> *Cellco Partnership d/b/a Verizon Wireless v. Global Information Group, Inc., et al.*, Order, No. 05-09757 (Fla. Circuit Ct., 13th Judicial Circuit, Hillsborough County, Nov. 2, 2005).

<sup>6</sup> *Cellco Partnership d/b/a Verizon Wireless v. Data Find Solutions, Inc., et al.*, Order, No. 06-CV-326 (SRC) (D.N.J., Jan. 31, 2006).

In addition to these suits, Verizon Wireless has taken a number of other steps to stop social engineering. Verizon Wireless has sent cease and desist letters to individuals operating data brokerage operations and encouraged the state attorneys general to pursue actions against social engineers. Verizon Wireless has assisted government law enforcement officers in identifying individuals involved in fraudulent activities. It has also supported federal legislation that would make obtaining CPNI by deceptive or fraudulent means a federal crime. On April 25, the House of Representatives, by unanimous vote, passed H.R. 4709, the “Telephone Records and Privacy Protection Act of 2006” which makes it a federal offense to obtain confidential phone records by false or fraudulent means, as well as to knowingly or intentionally purchase or sell such records.

All of these efforts are effective because they target the wrongdoers, and they focus on the methods used by pretexters. As detailed below, many of the specific proposals aim in the wrong direction because they would impose costs and burdens on carriers and their customers without effectively stopping pretexting.

### **III. THE FCC SHOULD REJECT MANY OF THE PROPOSALS IN THE NOTICE BECAUSE THEY WILL NOT STOP PRETEXTERS.**

The Commission seeks comment on a number of proposals, many from the *Petition*, including mandatory passcodes, an opt-in requirement for disclosure of CPNI to joint venture partners and independent contractors, audit trail requirements, encryption, customer notice of release of CPNI, verification rules, and limiting data retention. Given that the premise for the *Petition* and the *Notice* was to stop pretexting, Verizon Wireless opposes these proposals because they would be ineffective for this purpose and because of the burdens they would impose. Detailed new FCC rules that standardize carriers’ CPNI procedures may only make it easier for a pretexter who finds an effective way to

obtain CPNI to use it for many carriers.

**A. Mandatory Passcodes Would Burden Customers and Can Themselves Be Socially Engineered.**

EPIC claims that because common biographical data, such as a person's date of birth or social security number, is readily available in public databases, a consumer-set password would increase the security of CPNI.<sup>7</sup> The Commission seeks comment on this proposal, and in particular whether the Commission should require such a password system.<sup>8</sup> The Commission also asks whether the customer's ability to change a password would play into the hands of data brokers, and whether carriers should be required to notify customers that their password has changed.<sup>9</sup>

As Verizon Wireless detailed in its initial comments, passcode protection can be a valuable offering to customers who seek extra layers of protection beyond typical verification procedures to protect their CPNI. Verizon Wireless already provides this option to customers who desire to add this safeguard before their CPNI can be disclosed either by customer care or in-store personnel. If a subscriber sets up a passcode on his or her account, he or she must use the same passcode for on-line access. Verizon Wireless also provides a variety of extra protections for on-line access, including a requirement for customers to create a unique user name and password. To change his or her on-line password, a subscriber must answer a "challenge question" or a temporary password will only be sent to the customer's handset.

Although, as detailed in Section IV below, Verizon Wireless does not oppose including a passcode option for access to account information as part of an FCC safe

---

<sup>7</sup> *Notice* ¶ 15.

<sup>8</sup> *Id.* ¶ 16.

<sup>9</sup> *Id.*

harbor from enforcement, the Commission should not make passcodes mandatory. EPIC may be right that passcodes are more secure than social security numbers, but passcodes themselves can be obtained through fraudulent methods, and social engineers can obtain information without access to a customer's social security number or passcode. The problem with a rule mandating passcodes would be that for many customers, passcodes are not only not desired but would be a burden.<sup>10</sup> Customers often forget passcodes, and if not desired, passcodes could lead to a frustrating experience for a customer seeking answers to simple billing questions. Forcing tens of millions of customers to have passcodes to access their accounts would provoke customer complaints and would create additional systems requirements for carriers.<sup>11</sup> In short, although passcodes can be useful, they should remain an option because they are not completely effective for or desired by every customer. Rather than foist a mandate on every customer, the proper course is to allow carriers to make passcodes available to customers who desire them.

**B. The FCC Should Not Adopt an Opt-in Requirement for Disclosure of CPNI to Joint Venture Partners and Independent Contractors.**

The Commission requests comment on whether there is a greater possibility of dissemination of customers' private information in the context of CPNI disclosed to joint venture partners and independent contractors, and if so, whether the Commission should require carriers to obtain opt-in consent from a customer before disclosing CPNI to these

---

<sup>10</sup> Verizon cited a survey in its comments on EPIC's petition reporting that 87 percent of customers oppose mandatory passwords. Comments of Verizon, April 28, 2006.

<sup>11</sup> For example, on average, Verizon Wireless customers who have on-line accounts change on-line passwords about 30,000 times a day in total. Customers who do not have on-line accounts but have chosen to add passcodes change billing system passcodes a total of approximately 3,000 times a day. Given that only a small minority of Verizon Wireless customers have passcodes for access, forcing all customers to have them would generate literally tens of thousands of additional passcode changes daily.

types of providers. The Commission also references its safeguards applicable to the release of CPNI to joint venture partners and independent contractors and seeks comment on whether an opt-in requirement would better protect CPNI notwithstanding these safeguards.<sup>12</sup>

This proposal, like several others in the *Notice*, is a solution in search of a problem. Verizon Wireless has gathered information about data brokers' techniques in its preparation for litigation against these individuals. As discussed in Section II above, the typical method is for the pretexter to pose as another Verizon Wireless employee or a customer in order to try to obtain private customer information from a customer care employee who believes they are providing assistance. Verizon Wireless has no evidence that data brokers have obtained customer information from joint venture partners or independent contractors, which would make the type of consent applied to disclosure of customer information to these types of providers is irrelevant. Although it is theoretically possible for individuals to obtain access to information through joint venture partners and independent contractors, that risk is no greater for these entities. Moreover, joint venture partners and independent contractors do not typically have access to the type of information such as call detail that social engineers seek.

An opt-in requirement would provide no greater protection of customer information once it is in the hands of the joint venture partner or independent contractor, because the problem is not the misuse of CPNI by these entities, but the fraudulent access to CPNI by pretexters. Were opt-in consent required, pretexters would simply give that consent when procuring the CPNI they seek.

---

<sup>12</sup> *Id.*, ¶ 12.

Even if an opt-in requirement had any bearing on the likelihood of a social engineer to obtain a customer's information from a joint venture partner or independent contractor, which it does not, the Commission should not adopt such a requirement because it would violate the First Amendment. In the *US West* case, the Tenth Circuit applied the U.S. Supreme Court's four-part *Central Hudson* test to determine whether the FCC's original opt-in requirement was constitutional.<sup>13</sup> According to the third and fourth prongs of that standard, the government must show that the restriction on commercial speech directly and materially advances a substantial state interest and the regulation must be narrowly drawn.<sup>14</sup>

The Tenth Circuit concluded that the FCC did not demonstrate that its opt-in regulations directly and materially advanced its enumerated interests, particularly given the absence of a record of harm.<sup>15</sup> The court concluded that the opt-in requirement was not "narrowly tailored" because the agency had not demonstrated a sufficiently good fit between the means chosen (opt-in approval) and the desired statutory objectives (protecting privacy and competition), finding that the FCC had failed to adequately consider an "obvious and less restrictive alternative," an opt-out strategy.<sup>16</sup>

Following the appellate court's decision, the FCC adopted an opt-out rule, finding that it appropriately balanced the interests of carriers and customers. Replacing opt-out with an opt-in requirement now would resurrect precisely the same First Amendment problem that invalidated the FCC's original opt-in requirement. It would not promote the

---

<sup>13</sup> *US WEST v. FCC*, 182 F.3d 1224, 1233 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000). *See also Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of N.Y.*, 447 U.S. 557(1980) (*Central Hudson*).

<sup>14</sup> *Central Hudson*, 447 U.S. at 564-65. *See also US WEST*, 182 F.3d at 1233.

<sup>15</sup> *Id.*, 182 F.3d at 1235.

<sup>16</sup> *Id.*, 182 F.3d at 1238.

FCC's stated interest in protecting information from data brokers, let alone the direct and material advancement necessary to pass muster under the *Central Hudson* test. This is the case because, as stated above, there is no evidence to date that data brokers are obtaining information from joint venture partners and independent contractors as opposed to carrier employees. Moreover, given that the FCC's existing safeguards for disclosure of CPNI to joint venture partners and independent contractors have a direct impact on protecting such information from unauthorized disclosure, such a requirement would not be narrowly tailored as the law requires.

**C. Audit Trails Would Have Little Value Against Pretexting.**

EPIC asks the Commission to require carriers to record all instances when a customer's records have been accessed, whether information was disclosed, and to whom, claiming that this would deter company insiders from selling information and could help carriers to identify and investigate security breaches.<sup>17</sup> The Commission notes that 47 C.F.R. § 64.2009(c) requires carriers to maintain a record of instances when CPNI was disclosed to third parties, and seeks comment on whether to extend this rule to include disclosure of CPNI to account holders.<sup>18</sup>

The FCC previously adopted, but then removed, CPNI audit trail requirements.

When it repealed this requirement, the FCC stated:

We also agree with the petitioners, based upon the new evidence before us, that we should modify the *CPNI Order's* electronic audit trail requirements. This requirement was broadly intended to track access to a customer's CPNI account, recording whenever customer records are opened, by whom, and for what purpose. As AT&T points out, the *CPNI Order's* electronic audit trail

---

<sup>17</sup> *Petition* at 11.

<sup>18</sup> *Notice* ¶ 17.

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 regarding the use of CPNI are not violated we conclude that, on balance, such a potentially costly and burdensome rule does not justify the benefit.<sup>19</sup>

There is no reason for the Commission to reverse course by reimposing an audit trail mandate. First, there is no nexus between requiring audit trails and stopping pretexting, because no amount of recordkeeping after the fact will prevent a pretexter from obtaining CPNI.

Second, many carriers have developed their own recordkeeping procedures that are tailored to their own businesses. Verizon Wireless employs a variety of different tools that make a record of each individual who accesses a customer’s record in a system that customer service representatives use to interface with billing systems. Verizon Wireless also trains its customer service representatives to record when customer information is accessed, the subject of the discussion with the customer, and whether they have disclosed any information to the customer in the “notes” section of the customer’s account that is maintained as part of the billing system. These procedures would not appear to comply with the audit trail requirements that EPIC proposes. Verizon Wireless makes a record of which customer service representative performs certain transactions such as activations and feature additions, but it does not show in detail which screens are

---

<sup>19</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 272 of the Communications Act of 1934, as amended, *Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409, 14475 (1999).

accessed by a customer service representative.<sup>20</sup> These automated systems do not necessarily reveal whether information was disclosed and to whom. EPIC's proposal would therefore require Verizon Wireless to undertake costly systems changes to support enhancements to its systems.

Such systems enhancements, however, would not stop or even deter social engineers. As stated above, the primary means through which social engineers obtain information is via deceptive telephone conversations. Social engineers are con artists who are skillful at making customer care representatives believe that they are real customers who for some reason are in dire need of information about their accounts. Audit trails do not track oral communications between social engineers and customer service representatives, and as such would provide little value in the fight against these fraudulent actors. Because carriers could never be sure which calls were social engineering calls, to attempt to record all instances of social engineering, carriers would have to make a voice recording of and store for some period of time each and every call to customer service, which for Verizon Wireless can amount to as many as 10 million of calls each month. Likewise, the problem with expanding 47 C.F.R. § 64.2009(c) to include a recording of all instances in which CPNI is released to account holders is that it would require carriers to make recordings of every call because carriers release CPNI to customers virtually every time customers call to discuss their bill or calling plan – because the customers ask for such information or because it is necessary to answer the

---

<sup>20</sup> Verizon Wireless tracks the general category of information accessed by a customer service representative by category, representative, date, and time. Verizon Wireless also generates reports of accounts that are opened and viewed but for which there were no transactions on the account. Verizon Wireless also keeps track of each time a bill is retrieved by representative, date, time, and account number. None of these indicates whether information was provided to a caller.

customer's inquiry. Verizon Wireless estimates that merely recording each customer service call would cost approximately \$8 million per year. In addition, there would be considerable costs required in order to store tens of millions of calls.

**D. Encryption Requirements Would Not Deter Social Engineering.**

The Commission seeks comment on encryption, in particular whether carriers have evidence that data brokers are obtaining access to CPNI directly from databases and whether encrypting stored CPNI would be useful.<sup>21</sup> As detailed in its initial comments, Verizon Wireless uses encryption when it sends customer records to outside sources such as credit bureaus. Here again, however, Verizon Wireless is aware of no instances of “hacking” or that data brokers are obtaining access to customer information by intercepting e-mails containing such information. Moreover, encryption would not prevent social engineering because the data would have to be unencrypted before a customer service representative could access it. Encryption would thus be of no utility in stopping the kind of fraudulent conduct that triggered this proceeding. Again, the focus should be on aggressive law enforcement against the wrongdoer. The Commission should therefore not impose a requirement for carriers to encrypt specific data.

**E. The FCC Should Not Require Customer Notification.**

The Commission seeks comment on EPIC's proposal that companies notify customers when the security of their CPNI may have been breached and also whether certain types of requests should trigger advance notification.<sup>22</sup> For example, the Commission asks whether carriers should be required to take extra precautions to verify the authenticity of requests that data be sent somewhere other than the mailing address

---

<sup>21</sup> Notice ¶ 19.

<sup>22</sup> Notice ¶¶ 21-22.

where the account is registered, the e-mail address on file for the customer, or a telephone number listed on the customer's account.<sup>23</sup>

As Verizon Wireless stated in its initial comments, Verizon Wireless notifies its customers if it becomes aware of a security breach that has led to the disclosure of CPNI other than to the customer.<sup>24</sup> The FCC should not mandate an action that carriers already have the incentive to take to communicate with their customers. A requirement to notify customers that their security "may" have been breached should not be adopted. It would cause unnecessary distress and confusion for customers because the carrier would not necessarily be certain of the breach. Moreover, it would set an impossible compliance obligation because the carrier would not necessarily know that its notification obligation had been triggered.

With respect to advance notification prior to the release of CPNI, Verizon Wireless believes that if carriers follow adequate verification procedures to ensure that the customer is the account holder or authorized person on the account, advance notification is not necessary, and it would only delay customers' legitimate requests for information and be burdensome. Carriers' verification procedures are fundamental to protecting against the unauthorized release of information to data brokers, and it is for this reason that Verizon Wireless proposes that carriers must verify the identify of the person seeking CPNI before releasing it to fall within a safe harbor from enforcement.

Verizon Wireless also opposes a requirement to send a confirmation letter every time it discloses CPNI. This would entail generating a letter nearly every time a

---

<sup>23</sup> *Id.* ¶ 22.

<sup>24</sup> As Verizon Wireless stated in its initial comments, several states now require such notification. Verizon Wireless Comments at 8.

customer calls into Customer Service or inquires about bill, because CPNI is typically disclosed in these situations. This occurs millions of times each month at Verizon Wireless alone. Verizon Wireless estimates that a requirement to send such a confirmation letter would cost Verizon Wireless approximately \$70 million per year, making such an ineffective requirement unreasonable and prohibitively costly.

**F. Limiting Data Retention Would Not Impact Social Engineering and is Not Consistent With Certain Mandated Retention Requirements**

EPIC proposes that carriers eliminate call detail records after they are no longer needed for billing or dispute purposes.<sup>25</sup> EPIC does not specify a time that carriers should retain these records, but it also proposes that carriers should destroy or “deidentify” records after a certain period of time.<sup>26</sup> The Commission seeks comment on whether records should be deleted and, if so, how long such records should be kept.<sup>27</sup>

It is Verizon Wireless’s policy to keep customer records for seven years, but other carriers may have reasons to use longer or shorter periods. There is no reason to micromanage carrier practices in this way. Limiting data retention has no nexus to the problem at issue in this proceeding, which is primarily the practice of social engineers of calling customer care to obtain customer records. Social engineers do not trade in the type of old information that would be purged under EPIC’s proposal, nor do Verizon Wireless’s customer service representatives that are responding to requests for information have access to it.

Moreover, carriers often need to preserve this information to defend against complaints and to comply with court-ordered record retention directives. For example,

---

<sup>25</sup> *Petition* at 11-12.

<sup>26</sup> *Id.*

<sup>27</sup> *Notice* ¶ 20.

Verizon Wireless is involved in a putative nationwide class action lawsuit pending in California state court involving a host of historical challenges to its billing practices, including rounding up to the next full minute, and charging for incoming calls.<sup>28</sup> In 2002, in connection with this case and several other class actions from around the country that were consolidated into *Campbell* for class action settlement purposes, Verizon Wireless issued a document retention notice prohibiting the destruction of any billing data at issue in the litigation dating back to January 1, 1991. Past bills are relevant to the claims and defenses, especially damage issues, in this case as well as other litigation that may be brought against carriers. A rigid retention rule could impede carriers' legitimate need to preserve records to defend themselves in litigation. Given that there is no reason why such a rule would discourage pretexting, it should not be adopted.

#### **IV. VERIZON WIRELESS SUPPORTS TWO NEW RULES AND A SET OF PRACTICES THAT WOULD DEFINE A SAFE HARBOR FROM ENFORCEMENT.**

Because establishing detailed FCC rules in the areas discussed above would not curb social engineering, the Commission should instead adopt two new procedures, and establish a set of security requirements that if implemented would exempt a carrier from liability through a “safe harbor” from enforcement.<sup>29</sup>

##### **A. Carriers Should Post Their Privacy Policies and File CPNI Certifications With the Commission.**

Carriers should make clear to their customers how and when their information will be released and to whom. As set forth in its Privacy Principles posted on its web

---

<sup>28</sup> *Campbell v. AirTouch Cellular*, No. D044759 (Cal. Ct. of Appeal, Fourth App. Dist., Div. 1, March 24, 2006).

<sup>29</sup> *See Notice* ¶ 26.

site, Verizon Wireless has always been guided by strong codes governing the privacy of communications and information, and its Privacy Principles reflect its commitment and define its policy on safeguarding privacy. The company believes that its Principles strike a reasonable balance between customer concerns about privacy and those same customers' interest in receiving quality service and useful new products. The Principles give customers choice and flexibility regarding how their personal information is used, and they guide employees in handling customer information to ensure that private information remains private.

The Commission should require carriers to maintain and make available to all customers their privacy policies to inform customers about how information is collected and used, how customers can control how the information is used, and when and to whom it will be disclosed. This will provide customers vital information in their choice to do business with a carrier, and it would also provide the Commission with a way to learn about and track industry practices.

In addition, Verizon Wireless supports the Commission's proposal to require carriers to file their CPNI certifications required by 47 C.F.R. § 64.2009(e) with the Commission.<sup>30</sup> The proposal includes a requirement to attach an explanation of actions taken against data brokers and a summary of complaints received from customers concerning unauthorized release of CPNI.<sup>31</sup> Such a requirement would provide the Commission a greater ability to determine how carriers are complying with the FCC's rules and the extent of the data brokerage problem.

---

<sup>30</sup> *Id.* ¶ 29.

<sup>31</sup> *Id.*

**B. The Commission Should Adopt a Set of Procedures That if Implemented Would Be a Safe Harbor From FCC Enforcement.**

The Commission should in addition adopt a safe harbor similar to that contained in 47 C.F.R. 64.1200(c)(i) of its do-not-call rules. In that context, the FCC exempted a carrier from liability for telephone solicitations to individuals on the national do-not-call list if the carrier could demonstrate that the call was in error and that the carrier followed a set of routine business practices. These practices include written do not call compliance procedures, training of personnel, recording of a list of telephone numbers that the carrier may not contact, access to the national do-not-call database, and no use of the national do-not-call database for any other purpose than compliance with the FCC's rule.<sup>32</sup> The Commission reasoned that even where a carrier had careful procedures and had trained employees in compliance, given the volume of calls to customers, unlawful calls might inadvertently be made, and correctly determined that carriers should not be held liable for these isolated situations.<sup>33</sup>

The Commission's safe harbor policy for do-not-call violations makes equal sense for CPNI, because no matter how many rules and procedures carriers follow, a disclosure of CPNI could occur when a pretexter can circumvent those procedures. The disclosure would be due not to the inadvertent conduct of the carrier but the deception of an outside individual or entity. A safe harbor policy makes even more sense here because the prima

---

<sup>32</sup> 47 C.F.R. § 64.1200(c)(i).

<sup>33</sup> Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, *Report and Order*, FCC 03-153, CG Docket No. 02-278, July 3, 2003, at ¶38: "A seller or telemarketer acting on behalf of the seller that has made a good faith effort to provide consumers with an opportunity to exercise their do-not-call rights should not be liable for violations that result from an error." In the CPNI pretexting situation, the "violation" would result not from the carrier's error but from the deliberate deception of a third party, making a safe harbor even more appropriate.

facie violation is the product of a third party's fraudulent conduct. The Commission should establish a set of voluntary standards that carriers could comply with to avoid liability. This could include the following procedures that are specifically tailored to stop social engineers:

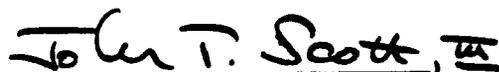
- Carriers must develop detailed written CPNI security procedures and conduct regular training of employees in the security of customer information.
- Carriers must verify that the account holder or an authorized party on the account is on the phone, in the store, or online. Verification procedures can and should vary, but each carrier should have such procedures in writing.
- Certain information should not be made available to individuals calling to request it, including the account holder. This could include the customer's social security number, tax identification number, and billing address.
- Carriers should enable customers to establish a passcode on their account for purposes of transactions over the phone, in the stores, and over the Internet. There should be an option for customers to reset the passcode if it is forgotten or lost.

## CONCLUSION

For the foregoing reasons, the FCC should not adopt the proposals contained in the *Petition* but should instead adopt specific disclosure rules and a set of best practices and procedures that if implemented would constitute a safe harbor from enforcement.

Respectfully submitted,

**VERIZON WIRELESS**

A handwritten signature in black ink that reads "John T. Scott, III". The signature is written in a cursive style and is underlined.

John T. Scott, III  
Charon H. Phillips  
1300 I Street, N.W.  
Suite 400 West  
Washington, D.C. 20005  
202-589-3740

April 28, 2006