

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;	)	
	)	
IP- Enabled Services	)	WC Docket No. 04-36
	)	
_____	)	

**COMMENTS OF VERIZON**

Michael E. Glover  
Of Counsel

Karen Zacharia  
Mark J. Montano  
VERIZON  
1515 N. Court House Road  
Suite 500  
Arlington, VA 22201-2909

Dated: July 9, 2007

Counsel for Verizon

## EXECUTIVE SUMMARY

The Commission's most recent CPNI Order requires carriers to take a number of steps to further protect CPNI, in general, and call detail information, in particular. Because there is nothing to suggest that these measures would not sufficiently safeguard CPNI from actions of data brokers and pretexters, the Commission should refrain from enacting additional regulations that could unnecessarily burden customers who have legitimate needs for accessing account information, but tend to dislike and forget passwords. In addition, the Commission should be mindful of the costs imposed by new regulations – including re-engineering systems and re-training employees – and avoid expensive, burdensome measures that increase the cost of service to customers while offering little or no data security benefit.

Accordingly, the Commission should not extend the requirement for a password for access to CPNI via customer-initiated calls beyond the disclosure of call detail information. Broadening the Commission's password requirement not only is unnecessary, but it would also run afoul of the First Amendment, which requires restrictions on speech to be narrowly crafted. Other requirements that the Commission previously rejected, such as audit trails and physical safeguards, including encryption, are no less burdensome today and continue to lack an obvious nexus to the prevention of pretexting. Similarly, there is no evidence that older and archived data has been a target of data brokers, and thus restricting carriers' data retention is unwarranted. Finally, any new regulations should not apply to business customers because these customers are able to negotiate the amount of CPNI protection that they require.

## TABLE OF CONTENTS

	Page
I. THE COMMISSION SHOULD REFRAIN FROM ADOPTING ADDITIONAL PASSWORD REQUIREMENTS FOR CPNI.....	3
A. The Burdens of Additional Password Requirements Far Outweigh Any Benefits. ....	3
B. Password Requirements for the Disclosure of CPNI Would Violate the First Amendment. ....	10
II. THE COMMISSION SHOULD CONTINUE TO REJECT BURDENSOME REQUIREMENTS THAT FAIL TO PROVIDE SUBSTANTIAL PROTECTION OF CPNI. ....	11
A. The Commission Has Twice Rejected a Requirement To Keep an Audit Trail of All CPNI Disclosures.....	11
B. The Commission Should Not Mandate Particular Physical Safeguards To Protect CPNI. ....	15
III. CARRIERS REQUIRE FLEXIBILITY IN THEIR DATA RETENTION PRACTICES TO MEET A VARIETY OF OBJECTIVES AND LEGAL REQUIREMENTS, INCLUDING PROTECTION OF CPNI. ....	17
IV. ANY NEW MEASURES DESIGNED TO PROTECT RESIDENTIAL CUSTOMER DATA SHOULD NOT BE EXTENDED TO BUSINESS CUSTOMERS.....	20
V. CONCLUSION.....	21

\*

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;	)	
	)	
IP- Enabled Services	)	WC Docket No. 04-36
	)	
	)	

---

**COMMENTS OF VERIZON<sup>1</sup>**

As it considers whether any additional changes to the recently pronounced CPNI rules may be appropriate, the Commission should exercise restraint in its approach. The new CPNI rules, which were released just three months ago, are quite far-reaching in scope and, as the Commission explained, will significantly strengthen its privacy rules and curtail pretexting. Because these rules have yet to take effect, much less prove ineffective, it is premature to conclude that additional CPNI safeguards would be necessary.

The Commission has sought comment on many of the same issues that Verizon and other commenters addressed just over a year ago. While the threat imposed by pretexters seems to have largely subsided due in part to new federal and state criminal statutes as well as carriers' enhanced data security measures, carriers need to maintain flexibility to continue to address any new fraudulent schemes or tactics employed by data brokers that may threaten the security of

---

<sup>1</sup> The Verizon companies participating in this filing ("Verizon") are the regulated, wholly owned subsidiaries of Verizon Communications Inc.

customer information.<sup>2</sup> The Commission should ensure that any new regulations do not deny carriers this flexibility.

At the same time, the Commission must continue to balance the need to protect customer data against other important business considerations. Public policy should reflect consumers' coexistent desires for strong privacy protections and ease in their transactions with the companies with whom they choose to do business. The Commission should be careful to avoid imposing unnecessary burdens on customers who have legitimate needs for accessing account information, but tend to forget passwords. In addition, it should be mindful of the costs imposed by new protections -- including re-engineering systems and re-training employees -- and avoid expensive, burdensome measures that increase the cost of service to customers while offering little or no data security benefit.

Applying these principles, the Commission should not add any new regulations since any potential privacy benefits resulting from further safeguards would fail to approach the burdens imposed on customers and carriers. Accordingly, the Commission should not extend the requirement for a password for access to CPNI via customer-initiated calls beyond the disclosure of call detail information. Broadening the password requirement would also violate the First Amendment, which requires restrictions on speech to be narrowly crafted. Other requirements that the Commission previously rejected, such as audit trails and physical safeguards, including encryption, are no less burdensome today and continue to lack an obvious nexus to the prevention of pretexting. Similarly, there is no evidence that older and archived data has been a target of data brokers, and thus restricting carriers' data retention is unwarranted. Finally, any

---

<sup>2</sup> Verizon uses the term "data brokers" to refer to persons who claim to be able to provide CPNI to others for a fee.

new regulations should not apply to business customers because these customers are able to negotiate the amount of CPNI protection that they require.

**I. THE COMMISSION SHOULD REFRAIN FROM ADOPTING ADDITIONAL PASSWORD REQUIREMENTS FOR CPNI.**

**A. The Burdens of Additional Password Requirements Far Outweigh Any Benefits.**

The Commission's recent Report and Order and Further Notice of Proposed Rulemaking attempts to "balance consumers' interests in ready access to their call detail, and carriers' interests in providing efficient customer service, with the public interest in maintaining the security and confidentiality of call detail information."<sup>3</sup> However, extending the password requirements to information other than call detail information accessed via customer-initiated calls would upset the Commission's delicate balance because the burdens on carriers and their customers would far outweigh any purported privacy benefits. No compelling evidence has arisen in the three months following the Commission's *2007 CPNI Order* that would support the Commission's reversing course and extending its password requirements.

In particular, requiring customers to provide a password before a service representative could provide *any* CPNI over the telephone would be frustrating to customers and unnecessarily burdensome. While there are undoubtedly others, Verizon can foresee two examples in which the requirement of a password for CPNI would yield significant customer harm by delaying or deterring legitimate transactions. One such legitimate transaction would be a customer's attempt to pay for service by telephone to avoid a late payment charge or the disconnection of his or her service for failure to pay. A customer may be aware of the existence of an outstanding balance, but may not know the exact balance nor have the bill, a late payment notice, or suspension notice

---

<sup>3</sup> Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 ¶ 17 (2007) ("*2007 CPNI Order*").

at hand. Since the balance of the bill would be encompassed by the definition of CPNI in 47 U.S.C. § 222(h)(1)(B) (assuming the balance concerns telephone exchange or toll service), the customer service representative could not inform the customer of the amount that he or she is required to pay unless the customer could provide a pre-established password. Issuing or resetting a password for that customer would be a time-consuming process that could delay payment past the date of disconnection. While such a disconnection could ultimately be reversed, both the customer and the carrier would face avoidable costs and inconvenience when other appropriate means of authentication could be utilized to provide the customer with his or her account balance.

Another legitimate transaction that would be unduly complicated or deterred would be a customer's efforts to change his or her package of services to another package that may result in savings. If a customer could not provide a password, the customer service representative could not discuss the customer's existing services. Again, issuing or resetting the password could cause a delay, which could cause the customer to continue in a more expensive plan longer than the customer wanted. In competitive markets, the time delay and additional costs to a customer could lead to a worsening of customer relations and possibly the loss of the customer.

As these scenarios demonstrate, in the estimation of many consumers, the added security benefit of a customer-set password for CPNI comes at too great a cost in terms of lost efficiency and convenience in conducting legitimate account transactions. The Commission understood this cost in its *2007 CPNI Order* when it observed that "many customers may not like passwords" and that "passwords can be lost or forgotten."<sup>4</sup>

---

<sup>4</sup> *Id.* ¶¶ 13 n.47, 16.

Third-party research confirms the Commission's understanding and demonstrates that passwords are not an appropriate security solution for all customers in all circumstances. For instance, according to a recent survey, 87 percent of customers asked about proposed legislation that would require some companies to mandate password protection were opposed to the idea of mandatory passwords.<sup>5</sup> Customers prefer having a choice of verifying their identity through passwords or through other objective identifiable personal data.<sup>6</sup>

Customers tend to dislike passwords because many customers regularly forget or misplace them; surveys have reported that more than 80 percent of people have forgotten their passwords.<sup>7</sup> Where a password is lost or forgotten, a customer must go through the process of resetting it. Some reports estimate that between 10 and 30 percent of help desk calls are for requests to reset passwords.<sup>8</sup> The business costs of addressing these password change requests

---

<sup>5</sup> See Larry Ponemon, "Perceptions About Passwords," BNA Privacy and Security Law Report (Mar. 6, 2006).

<sup>6</sup> *Id.* (69% of customers prefer the option of having company provide "a choice of password or the use of three pieces of personal data to verify identity," rather than requiring one or the other (data identification or password) be used by all customers (emphasis added)).

<sup>7</sup> See *id.* (88% of people surveyed had forgotten their password at least once in the past two years; 67% forgot their passwords three or more times in the past two years); see also Jason Hong et al., Attitudes and Behavior Towards Password Use on the Worldwide Web (Oct. 11, 2000) (almost 82% of people had forgotten a password established on a website), available at <http://www.passwordresearch.com/stats/study48.html>. For a link to various studies regarding passwords, see [www.passwordresearch.com](http://www.passwordresearch.com).

<sup>8</sup> See Axios Systems, Axios Systems Passwords Survey (Jan. 2003), available at <http://www.passwordresearch.com/stats/study68.html> (more than one third of the survey's respondents said that password problems represented between 40 and 60 percent of all help desk calls; another 22.5 percent said password issues accounted for between 20 and 40 percent of calls; 6.5 percent putting the figure at between 60 and 80 percent); The Cost of Forgotten Passwords (Mar. 25, 2004), available at <http://www.passwordresearch.com/stats/statistic162.html> (Cox Communications estimated that 20% of help desk calls were to reset passwords); Help Desk Institute 2004 Practices Survey (Nov. 2004), available at <http://www.passwordresearch.com/stats/statistic210.html> (more than 17% of help desk calls were for password resets – more than calls for desktop operating system or software support); Password Management, Single Sign-On, and Authentication Management

can be significant.<sup>9</sup> Moreover, the cost to the customer of resetting passwords – a process that increases the time required to conduct routine transactions and requires customer authentication through the same sorts of inquiries passwords are intended to replace – is not simply monetary. A customer making only occasional account inquiries who is compelled to re-set a password multiple times will be deterred from obtaining information about his or her own account. If the password is required before obtaining information from a customer service representative over the telephone, a mandatory password requirement will inevitably lead to increased call handling time. This is a source of frustration not only for the customer who may have trouble remembering a password but to all other customers in the queue, who would experience longer hold times.

While Verizon does not track data relating to forgotten passwords in the ordinary course, Verizon data that is available is consistent with the third-party research. For example, nearly three million attempted logins by residential online account users fail or are abandoned each year by users who cannot supply (or retrieve by answering a test question) the correct password and/or userID. The data suggest that Verizon would have to respond to over 6,000 calls per day if those users sought assistance to access their accounts. Furthermore, because customers with online access are more likely to be technologically savvy and thus more likely to recall

---

Infrastructure Products: Perspective (Jan. 7, 2002), *available at* <http://www.passwordresearch.com/stats/statistic167.html> (password requests account for 25% of help desk calls); Gartner Group, Password Reset: Self-Service That You Will Love (Apr. 15, 2002), *available at* <http://www.passwordresearch.com/stats/study76.html> (10% to 30% of help desk calls relate to password reset requests).

<sup>9</sup> Passwords Are Gobbling Up Your Profits (May 1, 2003), *available at* <http://www.passwordresearch.com/stats/statistic94.html> (2003) (reporting that it costs between \$100 to \$350 per user per year to manage passwords); Password Reset: Self-Service That You Will Love, *supra* (reporting password reset requests costs between \$51 to \$147 in labor costs); Citrix MetaFrame Password Manager (Sept. 2003), *available at* <http://www.passwordresearch.com/stats/statistic95.html> (password management costs estimated at \$250 per user per year).

passwords, the incidents of forgotten passwords would be exponentially higher if all customers were required to have a password before calling customer service and discussing CPNI.

In addition, requiring customer-set passwords could decrease the security of customer data. Confounded by password proliferation, many consumers afforded the option of establishing their own password re-use codes established for other purposes such as e-mail, credit card, or automatic teller machine access. And a large number of people admit to having shared their passwords with others.<sup>10</sup> Surveys also report that many users' passwords can be obtained simply by offering minimal inducements or using basic social engineering questions.<sup>11</sup> In the case of domestic disputes – which appear to be a common source of CPNI data broker problems – a disgruntled spouse or partner may have access to the customer's password and other identifying information.<sup>12</sup>

---

<sup>10</sup> See, e.g., Infosecurity Europe 2003 Information Security Survey (Apr. 2003), available at <http://www.passwordresearch.com/stats/study55.html> (two-thirds of workers surveyed had given their passwords to another colleague, and almost three quarters knew the passwords of another coworker).

<sup>11</sup> See, e.g., *id.* (people surveyed used common words or readily obtainable biographical data (such as birthdates or family names), and ninety percent of those surveyed gave away their computer password for a cheap pen); Infosecurity Europe 2004 Information Security Survey (Apr. 2004), available at <http://www.passwordresearch.com/stats/statistic120.html> (more than 70% of office workers surveyed “were willing to part with their password for a chocolate bar”; almost half of those surveyed said they would give their password to someone calling from the IT department, which left them “vulnerable to social engineering techniques,” as hackers often pretend to call from the IT department and request a user's log on and password to “resolve a network problem”).

<sup>12</sup> Testimony of Steve Largent, President and Chief Executive Officer, CTIA-The Wireless Association, Before the U.S. House of Representatives Committee on Energy and Commerce, at 3 (Feb. 1, 2006) (“We’ve had cases where the data brokers have possessed the customer password. We have had cases where they knew the date of birth of the customer and the full social security number. Because many of these cases seem to arise in divorce or domestic cases, it is common for a spouse to have all of the necessary identifying information long after a divorce or separation to obtain call records.”) (“CTIA House Testimony”), attached to Letter from Paul Garnett, CTIA, to Marlene H. Dortch, FCC, CC Docket No. 96-115, RM-11277 (Feb. 2, 2006).

Moreover, if the Commission were to require carriers to provide passwords to their entire embedded base of residential customers, whether directly or implicitly by requiring a password before the disclosure of any CPNI in response to customer-initiated calls, the costs would be substantial, likely many tens of millions of dollars. While some of Verizon's residential customers already have passwords, upwards of 20 million do not and would need to be issued passwords. For the majority of customers, the process of establishing a password would not be initiated until the customer needed access to his or her CPNI. At that time, the need to authenticate the customer and establish a password would complicate, and possibly deter, a legitimate transaction. The Commission has explicitly recognized the burden placed upon carriers in providing efficient customer service and customers in readily accessing their call detail due to password requirements in its *2007 CPNI Order*.<sup>13</sup>

It is clear that the costs and burdens on customers and carriers, many of which cannot be quantified, to establish and maintain passwords are considerable. While the Commission provided some alternatives to passwords in its *2007 CPNI Order*, the Commission's effort to "narrowly tailor[] [its] requirements to address the problem of pretexting" by limiting its password rules to the disclosure of call detail information<sup>14</sup> was by far the most effective at lessening the negative impact on customers and carriers. Removing that limitation and requiring customers who call a center to provide a password before a carrier discloses *any* CPNI would cause the burden of the CPNI regulations on carriers and customers to be overwhelming.

In addition, the benefits of a password requirement for non-call detail CPNI provided in response to customer-initiated calls are small. In its *2007 CPNI Order*, the Commission

---

<sup>13</sup> *2007 CPNI Order* ¶ 17.

<sup>14</sup> *Id.* ¶ 13 n.46.

correctly distinguished between the privacy interest (and the risk to that interest) of a customer’s call detail information and non-call detail CPNI. In particular, the Commission found that “the release of call detail over the telephone presents an *immediate risk* to privacy.”<sup>15</sup> The Commission’s *2007 CPNI Order* was “directly responsive to the actions of data brokers, or pretexters” to quickly obtain “private and personal information, including what calls were made to and/or from a particular telephone number and the duration of such calls.”<sup>16</sup>

By contrast, the release of non-call detail CPNI fails to present a similar “immediate risk to privacy.” Verizon is unaware of any systematic efforts to acquire non-call detail CPNI, such as a customer’s account balance or his or her service plan, through pretexting or similar deception. This makes sense because such information has little value to pretexters, particularly when compared to call detail records. In any event, no immediate risk to privacy exists because carriers, including Verizon, already have stringent authentication procedures in place that must be met before callers can access any non-call detail CPNI.

The Commission has further asked whether password protection might be appropriate for account changes, such as changing the address of record or billing methods. The Commission’s *2007 CPNI Order* already addresses this potential problem since carriers are required to notify customers “immediately” when an online account or address of record is created or changed.<sup>17</sup> The Commission should let carriers implement these rules before concluding they must do even more.

\* \* \*

---

<sup>15</sup> *Id.* ¶ 13 (emphasis added).

<sup>16</sup> *Id.* ¶ 2.

<sup>17</sup> *Id.* ¶ 24.

On balance, the burdens to both customers and carriers of password protection for non-call detail CPNI would outweigh any privacy benefits. The Commission's reasons set forth in its *2007 CPNI Order* for narrowly tailoring its password requirements to the pretexting problem continue to hold, and the Commission's conclusion should not be disturbed. Thus, password protection should apply, at most, to call detail information provided in response to customer-initiated calls.

**B. Password Requirements for the Disclosure of CPNI Would Violate the First Amendment.**

As Verizon has previously explained, additional password requirements directly interfere with speech between customers and carriers by forcing them to take required actions before carriers may communicate certain information to their customers.<sup>18</sup> Restrictions on what information can or cannot be communicated – whether through a mandatory password requirement, a requirement that carriers contact their customers via their home telephone regarding various issues, or other means – by their terms restrict speech and implicate the First Amendment. *See Verizon Nw., Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1191 (W.D. Wash. 2003) (striking down Washington's CPNI restrictions because “the regulations at issue here directly affect what can and cannot be said” and “[s]uch a restriction, no matter how indirect, implicates the First Amendment”).

Indeed, requiring passwords for the disclosure of all CPNI necessarily would restrict customers' ability to obtain information that they want from their service provider and carriers' ability to provide information they desire to provide to their customers. *See, e.g., U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1232 (10<sup>th</sup> Cir. 1999) (“Effective speech has two components: a speaker

---

<sup>18</sup> *See Requiring “Opt-In” Prior to Sharing CPNI with Marketing Vendors: Unconstitutional and Unwise*, white paper attached to Verizon letter, CC Docket No. 96-115, (Jan. 29, 2007); Verizon letter, CC Docket No. 96-115 (Dec. 22, 2006).

and an audience. A restriction on either of these components is a restriction on speech.”); *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 756-57 (1976) (explaining that communications are protected under the First Amendment whether the restriction is applied at the source or impedes the listener’s reciprocal right to hear the communication).

Just as a restriction on a carrier’s ability to speak can violate the First Amendment, so too can a barrier to a customer’s willing receipt of speech. *See, e.g., Project 80’s, Inc. v. City of Pocatello*, 942 F.2d 635, 639 (1991); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965) (“We rest on the narrow ground that the addressee in order to receive his mail must request in writing that it be delivered. This amounts in our judgment to an unconstitutional abridgement of the addressee’s First Amendment rights. The addressee carries an affirmative obligation which we do not think the Government may impose on him.”).

Because any password requirements will restrict speech, they are subject to a heightened constitutional scrutiny under the First Amendment. Regardless of whether a particular restriction is ultimately deemed to be content-based or not, or to apply in a given case to commercial or non-commercial speech, any such restriction must at a minimum be crafted narrowly and restrict no more speech than is necessary. Requiring a password for the disclosure of all CPNI – rather than just the subset of CPNI that presents an “immediate risk to privacy” – would fail that test.

**II. THE COMMISSION SHOULD CONTINUE TO REJECT BURDENSOME REQUIREMENTS THAT FAIL TO PROVIDE SUBSTANTIAL PROTECTION OF CPNI.**

**A. The Commission Has Twice Rejected a Requirement To Keep an Audit Trail of All CPNI Disclosures.**

The Commission should not adopt stringent audit trail requirements in this proceeding for the same reason the Commission has rejected them in the past: such requirements are not closely

targeted to protecting CPNI and are inordinately expensive. In its 2006 Notice of Proposed Rulemaking, the Commission sought comments as to whether the benefits of audit trails might justify the burdens on carriers.<sup>19</sup> After reviewing the comments, the Commission decided not to mandate audit trails; instead, the Commission required carriers to “determine what specific measures will best enable them to ensure compliance” with their duty to take reasonable measures to discover and protect against improper attempts to obtain CPNI.<sup>20</sup> The Commission reasoned that providing carriers with the flexibility to meet their statutory duty would allow them to “improve security of CPNI in the most efficient manner possible and better enable small businesses to comply with [the Commission’s] rules.”<sup>21</sup>

The Commission previously adopted an audit trail requirement in 1998<sup>22</sup> but quickly reversed itself on reconsideration when the industry pointed out the enormous costs to modify systems to meet the requirements and to maintain the necessary databases to track this information.<sup>23</sup> Indeed, the Commission cited an estimate from one carrier that it alone would have to spend more than \$270 million to comply with the new rule.<sup>24</sup> A number of other commenters warned that the audit trail requirement would be “particularly burdensome for small

---

<sup>19</sup> Notice of Proposed Rulemaking, 21 FCC Rcd 1782 ¶ 18 (2006) (“2006 Notice”).

<sup>20</sup> 2007 CPNI Order ¶¶ 33-34; *see id.* ¶ 64 (“For instance, and as discussed above, although we decline to impose audit trail obligations on carriers at this time, we expect carriers through audits or other measures to take reasonable measures to discover and protect against activity that is indicative of pretexting.”).

<sup>21</sup> *Id.* ¶ 34.

<sup>22</sup> In the *Second Report and Order* the Commission mandated audit trails in order to encourage carrier compliance and to create a method of verification where disputes arose. *See Second Report and Order and Further Notice of Proposed Rulemaking*, 13 FCC Rcd 8061 (1998).

<sup>23</sup> Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409 ¶ 127 (1999) (“*Reconsideration Order*”).

<sup>24</sup> *Id.* ¶ 124.

and rural carriers.”<sup>25</sup> On reconsideration, the Commission recognized that the audit trail requirement was “a potentially costly and burdensome rule [that] does not justify its benefit.”<sup>26</sup> As in the Commission’s 2007 CPNI Order, the *Reconsideration Order* acknowledged that existing rules already required carriers to protect CPNI and that carriers had existing internal procedures to do so.<sup>27</sup> The same is still true today, and Verizon is aware of no significant technological changes that would suddenly make audit trails feasible.

As the Commission has previously concluded, the costs in money and time to obtain, record, and archive *detailed* information about each of these calls – including the specific customer data accessed or disclosed – are substantial. It would require re-engineering systems and company-wide re-training, an exceedingly costly and time-consuming proposition. It would also significantly increase the time for handling customer calls if a representative were required to record every customer record accessed whenever responding to a customer request for information.

The collection and storage of such data would be crippling to carriers because the volume of potential data that would have to be tracked is enormous. Verizon, for example, handles, on average, more than 400,000 residential customer calls per business *day*. The customer service representatives are trained to provide a customer with information pertaining to a new service or services that a customer may value, which means the vast majority of those calls would require the disclosure of CPNI. Similarly, Verizon receives over 40 million customer online logins per year.

---

<sup>25</sup> *Id.* ¶ 125.

<sup>26</sup> *Id.* ¶ 127.

<sup>27</sup> *Id.*

In addition, adopting audit trail requirements likely would provide only limited benefits in addressing the data broker problem. It appears that in most cases, data brokers obtain confidential customer data by pretending to be someone who can legitimately access customer data.<sup>28</sup> Indeed, as the Commission acknowledges at the beginning of the *2007 CPNI Order*, the very impetus behind the proceeding is to respond to pretexting.<sup>29</sup> If pretexting is the data brokers' primary means of obtaining customer data (and there is no reason to believe otherwise), then an audit trail may reveal only that someone purporting to be the customer called and asked about customer detail – something that would not be helpful in preventing data broker access to such records or tracking the wrongdoer to a specific person.

Finally, the benefits of audit trails may be obtained in a less costly manner. While Verizon is reluctant to publicly detail its CPNI security processes for fear of educating data brokers, Verizon has developed tools to prevent improper access attempts and assist in the detection of a pattern of improper access attempts in both the call center and online settings.

These current practices, which address the rationale expressed by EPIC for an audit trail requirement in its Comments to the Commission's prior Notice<sup>30</sup> at a fraction of the cost, demonstrate that the Commission's flexible approach set forth in the *2007 CPNI Order* works in

---

<sup>28</sup> See, e.g., Written Statement of Kris Anne Monteith, Chief, Enforcement Bureau, FCC, Before the Subcommittee on Consumer Affairs, Product Safety, and Insurance Committee on Commerce, Science and Transportation, United States Senate, on "Protecting Consumers' Phone Records," <http://www.fcc.gov/ola/docs/monteith020106.pdf>, at 5 (Feb. 8, 2006) ("The carriers [that spoke with the FCC Enforcement Bureau staff] generally expressed their belief that the problems they have experienced in this area are largely, if not exclusively, related to attempts by individuals outside the company to obtain information through pretexting, rather than by 'rogue' employees selling information to data brokers."); CTIA House Testimony, at 2 ("Overwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of 'pretexting,' which is nothing more than lying to obtain something you aren't entitled to procure lawfully.").

<sup>29</sup> *2007 CPNI Order* ¶ 2.

<sup>30</sup> EPIC Comments at 13 (Apr. 14, 2006).

practice. Accordingly, an audit trail containing detailed records of all CPNI access provides little, if any, additional benefit to the protections the FCC already adopted in the *2007 CPNI Order*.

**B. The Commission Should Not Mandate Particular Physical Safeguards To Protect CPNI.**

As with audit trails, the Commission should permit carriers to determine what specific physical safeguards would best enable them to ensure compliance with their duty to take reasonable measures to discover and protect against improper attempts to obtain CPNI. In its *2006 Notice*, the Commission sought comments as to whether the benefits of one physical safeguard – encryption – might justify the burdens on carriers.<sup>31</sup> In its *2007 CPNI Order*, the Commission concluded that it was unnecessary to require encryption of CPNI given carriers' general duty to protect CPNI. Specifically, the Commission stated, “[A]lthough we do not specifically require carriers to encrypt their customers’ CPNI, we expect a carrier to encrypt its CPNI databases if doing so would provide significant additional protection against the unauthorized access to CPNI at a cost that is reasonable given the technology a carrier already has implemented.”<sup>32</sup> Recognizing the significant cost of encryption, the Commission observed that it may not be necessary, but “if carriers begin to experience increased attempts to obtain CPNI through hacking or similar measures, we would expect all carriers to revisit whether encryption of CPNI databases would satisfy their obligation to take reasonable steps to protect CPNI databases from unauthorized third-party access.”<sup>33</sup> The Commission should resist any

---

<sup>31</sup> *2006 Notice* ¶ 19.

<sup>32</sup> *2007 CPNI Order* ¶ 64; *see* ¶ 36 (“[A]lthough we decline at this time specifically to require carriers to encrypt their CPNI databases, we interpret Section 222 as requiring carriers to protect CPNI when it is stored in a carrier’s database.”).

<sup>33</sup> *Id.* ¶ 36 n.116.

proposals to retreat from the flexible approach espoused in its *2007 CPNI Order* for encryption and apply it to all other physical safeguards.

With respect to encryption, Verizon currently encrypts data in a variety of circumstances, including certain electronic transmissions of data to its affiliates and third parties authorized to access or maintain CPNI, to protect confidential data.<sup>34</sup> Even so, the cost of encrypting *all* CPNI located in all of Verizon's systems would likely be many tens of millions of dollars, presuming "encryption" means the Advanced Encryption Standard ("AES") adopted by the National Institute of Standards and Technology. Yet encryption offers no guarantee of security. Sophisticated hackers with resources and time could theoretically penetrate encrypted databases – a problem not unique to telecommunications but faced by every industry that handles electronically-stored sensitive data.

Moreover, there is no evidence to suggest that the unauthorized release of customer data is caused by data brokers hacking into carriers' systems. Again, it appears that data brokers proceed by deceit and impersonation through pretexting or social engineering, fraudulently convincing customer service personnel that they have authorized access to an account. Encryption of data within a carrier's internal database is no protection when a customer service representative believes he or she is speaking with an authorized account holder and will therefore release CPNI whether it had previously been encrypted or not. A requirement to encrypt records would impose significant costs that cannot be justified, particularly in the absence of any demonstrated benefit in deterring data brokers or enhancing security beyond its current level.

In addition to its routine use of encryption, Verizon employs a number of physical safeguards that protect CPNI from improper disclosure. A small sample is listed below:

---

<sup>34</sup> See Verizon, *Privacy and Customer Security Policies* (Jan. 2005), available at <http://www22.verizon.com/about/privacy/customer/>.

- Verizon’s call center systems and databases employ access controls. Only authorized personnel may access these systems and only in appropriate circumstances.
- Physical access to Verizon call centers is protected via identification passcards.
- Verizon employs a variety of protective measures in data centers where CPNI is stored, including identification cards, electronic entry, security guards, and security cameras.
- Verizon requires CPNI-specific training for its employees that have access to CPNI. In addition, all employees are trained on Verizon’s Code of Business Conduct, which includes Verizon’s privacy principles and addresses the proper handling of confidential customer information.
- Verizon also transmits certain data through a secure, dedicated service, where third parties are physically restricted from accessing the network.

Consistent with audit trails and encryption, the Commission should give carriers flexibility in determining which other physical safeguards may or may not be reasonable in light of carriers’ duty to protect CPNI. Adopting a rigid set of rules would not provide the efficient level of CPNI protection in the long run, particularly where threats to the data are constantly evolving. Nor is there reason to change course until the Commission’s new rules are tested.

**III. CARRIERS REQUIRE FLEXIBILITY IN THEIR DATA RETENTION PRACTICES TO MEET A VARIETY OF OBJECTIVES AND LEGAL REQUIREMENTS, INCLUDING PROTECTION OF CPNI.**

In its *2006 Notice*, the Commission sought comments as to whether CPNI records should be deleted, and, if so, how long such records should be kept.<sup>35</sup> The Commission did not reach a

---

<sup>35</sup> *2006 Notice* ¶ 20.

conclusion on this issue and therefore has requested further comments “in light of the rules [the Commission] adopt[s] in this Order and the recent enactment of criminal penalties against pretexters.”<sup>36</sup>

As an initial matter, regardless of the Commission’s and Congress’ recent attempts to further protect CPNI, the Commission should not require carriers to delete call records when they are no longer necessary for billing or dispute purposes or, alternatively, require that carriers “de-identify” records, i.e., separate data that identify a particular caller from the general transaction records. Suggestions to delete these records fail to recognize that carriers retain customer records containing CPNI for a variety of reasons unrelated to billing and disputes. Such records are frequently needed and retained in the usual course of business for use in civil and criminal litigation. They also are regularly used to respond directly to customer inquiries<sup>37</sup> and for fraud detection and follow-up investigations. Furthermore, under the Fair Credit Reporting Act, creditors are required to respond to a credit reporting dispute by investigating its records and responding. For a telephone company, those records are generally invoices or call detail information stored electronically that can be generated into a readable document. If the creditor cannot establish that a reported delinquency is valid, if for example, the creditor was required to delete the data records, it must delete the delinquency from reporting. Reported delinquencies stay on a consumer’s credit report for seven years, and the consumer could dispute a charge years after the delinquency was first reported.

---

<sup>36</sup> 2007 CPNI Order ¶ 71.

<sup>37</sup> Customers often request this information to determine whether they are on the appropriate plan, divide up monthly charges in a roommate situation, and a variety of other reasons.

Even the FCC's rules contain data retention requirements that may be at odds with those proposed by EPIC in 2006. For example, EPIC's deletion plan, which imposes a strict deletion rule when data is no longer needed for billing purposes or disputes, may be contrary to the Commission's Part 42 rules requiring that carriers retain telephone toll records for 18 months<sup>38</sup> and all other records for the period established in the carrier's data retention index.<sup>39</sup> Even after the customer has left the company, there may be a number of reasons why a carrier may lawfully access the customer's information, such as to respond to law enforcement requests, to engage in "winback" campaigns or other proper marketing uses, or to address potential allegations of slamming.<sup>40</sup> Moreover, there is no evidence that older records are more susceptible to fraudulent disclosure than newer ones.<sup>41</sup> Therefore, there is no reason to require carriers to delete customer records containing CPNI prior to the date specified under the company's existing document deletion schedule or when the statute of limitations has run on any potential dispute.<sup>42</sup>

If the Commission is correct that its *2007 CPNI Order* "strengthen[s] [its] privacy rules by adopting additional safeguards to protect customers' CPNI against unauthorized access and disclosure" and "will sharply limit pretexters' ability to obtain unauthorized access,"<sup>43</sup>

---

<sup>38</sup> 47 C.F.R. § 42.6.

<sup>39</sup> 47 C.F.R. § 42.7.

<sup>40</sup> See *Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409, ¶¶ 66-74 (1999) (eliminating the rule prohibiting the use of CPNI in winback campaigns); 47 C.F.R. § 64.1100 *et seq.* (subjecting telecommunications carriers to obligations regarding subscribers' change of telecommunications provider).

<sup>41</sup> See *CTIA Comments*, CC Docket No. 96-115, at 19-20 (Oct. 31, 2005).

<sup>42</sup> As with required encryption, the costs of de-identifying CPNI would likely be many tens of millions of dollars. Although de-identification implies less specific standards than encryption, the costs associated with de-identification are largely the same as those for encryption because logical and physical modifications to the database schema are required.

<sup>43</sup> *2007 CPNI Order* ¶¶ 1-2.

restrictions on a carrier's retention of CPNI cannot be justified. Congress' recent enactment of the Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039, which explicitly bans pretexting and selling or transferring confidential phone records information, as well as numerous other newly enacted state statutes that criminalize pretexting further call into question the necessity of limiting a carrier's retention of CPNI. Obviously, if pretexters' access to recent CPNI is barred and/or deterred, then both current and historical data are no longer at risk.

**IV. ANY NEW MEASURES DESIGNED TO PROTECT RESIDENTIAL CUSTOMER DATA SHOULD NOT BE EXTENDED TO BUSINESS CUSTOMERS.**

To the extent the Commission decides to implement additional regulations, they should be limited to residential customers. The Commission recognized in its *2007 CPNI Order* that business and residential customers do not share the same privacy risks and concerns when it set forth the "Business Customer Exception."<sup>44</sup> The exception to the Commission's "carrier authentication rules" applies to business customers whose carrier contract is serviced by a dedicated account representative as the primary contact and specifically addresses the carrier's protection of CPNI.<sup>45</sup>

The exception is too narrow to substantially lessen the burdens on a carrier for two reasons. First, the exception should apply to all business customers that negotiate service contracts with carriers, rather than just those that have a dedicated account representative. Even business customers that do not have a dedicated account representative are sophisticated and tend to employ counsel and/or consultants to represent their interests. It is unreasonable to assume that businesses would be unable to contract for the CPNI protection that they desired. Second,

---

<sup>44</sup> *Id.* ¶ 25.

<sup>45</sup> *Id.*

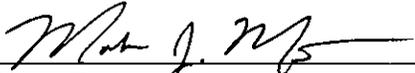
the exception should apply to more than just the Commission's "carrier authentication rules." If, for example, the Commission enacts rules in this proceeding relating to audit trails, physical safeguards, and/or data retention, these rules should not apply to a carrier's business customers that are well able to negotiate for this protection themselves.

A broader exception would take into account the uncontroverted fact that the data broker problem is targeted primarily at residential customer data. Many business customers employ their own security solutions and would not need, nor want to pay for, additional security protections tailored for the data broker problem affecting residential customers. Business customers often have a greater need for efficiency and convenience in receiving information about their accounts because their bills tend to be larger and may require more detailed review than residential customer accounts. Because of these significant differences, the Commission should leave the suitable level of CPNI protection to whatever carriers and their business customers agree upon.

## **V. CONCLUSION**

The Commission should evaluate the efficacy of its newly enacted rules before issuing potentially burdensome additional requirements that add little or no data security benefit. In particular, the agency should reject proposals to require: (1) passwords for non-call detail CPNI provided in response to customer-initiated calls; (2) audit trails; (3) encryption; and (4) data deletion after a certain time. Should the Commission determine that any regulations on one or more of these topics would be appropriate, the Commission should exclude business customers.

Respectfully submitted,

By:  \_\_\_\_\_

Karen Zacharia

Mark J. Montano

VERIZON

1515 N. Court House Road

Suite 500

Arlington, VA 22201-2909

703.351.3039

Of Counsel  
Michael E. Glover

Counsel for Verizon

Dated: July 9, 2007