

Donna Epps  
Vice President  
Federal Regulatory



1300 I Street, NW, Suite 400 West  
Washington, DC 20005

Phone 202 515-2527  
Fax 202 336-7922  
donna.m.epps@verizon.com

December 22, 2006

**Ex Parte  
Via ECFS**

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> St., S.W.  
Washington, DC 20554

**Re: *Ex Parte* Notice in CC Docket No. 96-115 – Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; and RM-11277 – Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information**

Dear Ms. Dortch:

This letter explains why Verizon<sup>1</sup> anticipates that it take 12 to 18 months to complete implementation of new CPNI safeguarding rules now being contemplated by the Commission, depending on the specifics, and why any new rules should not apply to wireline business customers.

Before explaining why the IT systems development work and customer representative training will take 12 to 18 months, Verizon reiterates here its strong support for the Commission’s goal of preventing pretexting and protecting confidential customer data against unauthorized release. Indeed, Verizon has safeguards and procedures in place for guarding against improper disclosure or theft of customer information. We review and modify these procedures on a regular basis to minimize the possibility of improper disclosure of customer information while at the same time providing quality service to our customers. Consistent with this commitment to customer privacy, Verizon and Verizon Wireless have jointly proposed in this docket specific rules that would improve safeguarding of consumer data without burdening legitimate access by our customers. *See* Letter from Donna Epps on behalf of Verizon and Verizon Wireless, to Marlene

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

H. Dortch, Federal Communications Commission, CC Docket No. 96-115, RM-11277 (filed Dec. 14, 2006). If the Commission concludes that it must implement new CPNI rules, we encourage the Commission to use those draft rules as the basis for any requirements.

As Verizon and other commenters have stated, mandatory passwords are not a panacea against pretexting. The new CPNI rules should therefore take the form of a safe harbor, so that carriers that adopt and implement reasonable practices and procedures consistent with those rules would not be subject to penalties as long as they implement certain security procedures.

Verizon does not know what specific rules the Commission will adopt or what new requirements may be imposed, but, for the purposes of this *ex parte*, Verizon has made certain assumptions in order to develop an expected timeline for implementation. If the Commission adopts rules that contain requirements different than the assumptions contained herein, the implementation timeline will accordingly be different. In making these assumptions, Verizon does not necessarily recommend them or urge their adoption as part of new and broader CPNI rules. In fact, as we have explained elsewhere, if the Commission intends to adopt new rules, it should adopt the safe harbor proposal filed jointly by Verizon and Verizon Wireless. This proposal appropriately balances customers' needs for ready access to their accounts with the public interest in the privacy of those accounts.

Whether or not the Commission adopts such a safe harbor, the Commission must afford carriers and their customers an adequate time to make the necessary systems changes, train customer service representatives, and take other required action without disruption of ongoing operations. As explained in greater detail below, Verizon estimates that it will need 12 to 18 months to create new databases to house millions of new passwords, perform the IT programming and code work necessary to access and manage such massive databases, modify existing systems to comply with the Commission's order, train Verizon's nearly 10,000 customer service representatives on how to assist customers in setting up passwords, and migrate more than 12 million online account customers through a re-initialization process.

In addition, it is critical that any new safeguarding practices not apply to business wireline customer accounts. There is no evidence that pretexters have targeted wireline business customers or their call records. In addition, account representatives typically serve wireline business accounts instead of customer service centers, making procedures that govern calls to customer service centers irrelevant for these customers.

**1. Implementing new requirements will require Verizon to reconfigure its billing systems and perhaps implement entirely new authentication platforms, train nearly 10,000 customer service representatives, and notify millions of wireline customers. The Commission should therefore allow 12 to 18 months for carriers to achieve compliance.**

Based on some parties' filings in this docket, Verizon understands that the Commission may be considering several requirements, including a requirement that call detail records not be

released over the telephone unless the customer provides a password,<sup>2</sup> a requirement for online accounts to be reinitialized, and the implementation of additional verification procedures.

Verizon estimates that it needs 12 to 18 months to implement these types of changes, depending on the specifics. Verizon would need to perform the necessary systems modifications, software development and programming, and field testing before changes could be implemented across the Verizon footprint for our 32 million residential landline customers and 12 million online accounts. In addition, Verizon must perform activities necessary to notify *all* of its residential customers, adopt new methods and procedures, and train Verizon's approximately 10,000 consumer customer service representatives.

The first step in this effort would be to develop appropriate business requirements to implement all the new requirements and new password practices, a process that can take several months. Verizon's IT organization then must translate those requirements into systems, software, and network requirements. New functions and software must be written, programmed, tested in the Verizon labs, and then implemented in the field. This process is known as an IT "release," and "major releases" typically occur every other month. Business requirements that are too large for a single release must be performed in discrete parts and therefore are usually spread out over several releases. For the large and complex systems used to support Verizon's telecom operations, the scheduling (and contents) for a given release is often established months in advance. While adjustments and reprioritization are made after release scheduling is established, such changes may impact other components of that same release or significantly disrupt implementation of features, functions, and fixes planned to occur across multiple releases.

As we explained above, Verizon does not know what any new requirements might be. Based on the assumptions described above, however, Verizon anticipates that implementing and supporting the re-initialization process will take the most significant amount of IT work, with the development of IT application changes or a new authentication platform for call detail requests consuming the next largest segment of IT effort (with the associated scheduling impact). For example, if the Commission were to require re-initialization for online accounts, Verizon would have to create new passcodes for all of its online accounts, notify customers of these new passcodes, modify its IT systems to recognize the new passcodes, and modify its IT systems to block all CPNI or call detail records after the prescribed period of time for customers who do not use the new passcode. Verizon estimates that developing systems and programming changes to implement these new requirements would be a major change and would probably need to be spread out over several IT major releases, which could take 8 to 12 months to implement.

---

<sup>2</sup> Verizon assumes that an order would also require Verizon to obtain a password from customers prior to the release of call detail records or any CPNI online. Since Verizon already requires a password in these situations, Verizon assumes no additional work will be necessary to implement this specific requirement.

Like any other project, the presence of software or programming “bugs” may delay a scheduled release and send the project back to the lab for further testing and development work. Any implementation schedule, therefore, must leave time for fixing any problems that are discovered during testing.

Finally, Verizon would prefer to make these changes in certain ways to ensure customer satisfaction is maintained during the implementation of any systems changes. Verizon would like to conduct a pilot of the new processes in a limited geographic scope. In addition, a release like this that will impact a large customer base should be phased in over several months. Online customers are likely to call our service representatives with questions about the new processes, and, if all those customers call the centers in the same time period, the centers will be flooded with calls and will not be able to provide quality customer service. We believe that the risks to our customers of account access disruption or other adverse customer impact, resulting from a compressed timeframe for migration to these new processes and procedures, are much greater than the risks associated with pretexting. A 12- to 18-month period would allow Verizon to implement these rules with a minimum of adverse impact to its customers or its operations.

In addition, Verizon must also train its 10,000 customer service representatives on any new business practices. This, too, is a time-consuming process. The lines of business translate these practices into various documents for the customer service representatives. This includes slides and presentation documents, notices, and scripts for use during calls with customers. Senior managers then must train the trainers, who in turn train, evaluate, and observe Verizon’s 10,000 customer service representatives implementing the new business rules. Sometimes the business rules are complicated, and customer service representatives must be re-trained to ensure compliance. Additionally, the training must be phased in over time to ensure that Verizon can continue to care for customer calls into the call centers and avoid excessive wait times. As a result, training is normally spread out over several weeks for each call center. Verizon has multiple call centers across the country, and this staggered training would take place over the course of several months to cover all call centers.

Aside from the work to develop new systems and software and train customer service representatives, Verizon would also need to notify millions of customers in a verifiable manner about any new password practices. The time to prepare and mail letters to Verizon’s approximately 32 million wireline residential customers alone could take four or more months. This includes the time to prepare the text, generate the mailing list, perform a “mail merge” for tens of millions of letters, and handle letters that are returned for one reason or another. Because of the size of Verizon’s wireline consumer customer base, even extraordinary outreach measures undertaken at great expense may not reach many consumers.

**2. Any new rules concerning protection of the CPNI of wireline customers should not apply to wireline business and enterprise customers.**

Any new Commission rules should allow carriers and their customers the ability to tailor privacy solutions to best meet customers’ needs. In particular, the Commission’s rules should

Ms. Marlene H. Dortch

December 22, 2006

Page 5

recognize that the data brokers do not target business wireline customers. Many wireline business customers have their own security solutions and will not need additional security protections tailored for the data broker problem affecting residential customers. Wireline 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. Finally, unnecessarily sweeping business/enterprise customers into the scope of these new rules could have an unintended adverse impact on security and privacy. Even something as simple as a requirement to use the "billing address" as part of notification or re-initialization can cause problems. For example, businesses often have designated customer employees to handling account changes for them, and those employees are typically not in the same part of the enterprise as the accounts receivable personnel, who are assigned to receive and pay bills. Accordingly, a rule directing a provider to send a new password to the "billing address" would, in effect, afford the accounts receivable personnel with far greater rights than the business customer intends. The above discussion does not, of course, address every potential complication that would arise from application of these rules to business. Rather, our intent is to present evidence of the different process, risks, and needs associated with business customers and the complexity of attempting to cover business customers in the pending rules.

\* \* \* \* \*

We welcome the opportunity to discuss these issues further. Please do not hesitate to contact us if you have any questions.

Respectfully submitted,

A handwritten signature in black ink that reads "Donna Epps". The signature is written in a cursive, flowing style.