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

February 23, 2007

Ex Parte

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Implementation of the Telecommunications Act of 1996-Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information, CC Docket No. 96-115; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, RM 11277

Dear Ms. Dortch:

In considering what an appropriate timeline is for implementing any new CPNI safeguarding rules that may be adopted here, the Commission should weigh the importance of getting new safeguards in place against the importance of doing so in a way that will minimize customer frustration and confusion. When the Commission adopted the original CPNI rules, it acknowledged that carriers cannot modify IT systems and other operational systems immediately, and it thus gave carriers eight months to implement rules that would require those changes. A similar phase-in period is needed here because the notification and authentication requirements being considered would also require IT systems and other operational systems changes, as detailed below. At a minimum, six months is the least amount of time the Commission should adopt for changes as extensive as those it is considering here. Anything shorter will not provide enough time to educate customers about changes and for carriers to conduct the necessary training and information technology systems development work.

In this *ex parte*, we discuss the steps Verizon[1] will need to take to implement several of the CPNI safeguards that we understand the Commission is considering:[2]

---

[1] The Verizon companies participating in this filing ("Verizon") are the regulated, wholly owned subsidiaries of Verizon Communications Inc.

[2] As we have explained previously, Verizon has had to make certain assumptions about what safeguards the Commission may impose, but Verizon does not recommend them or urge their adoption as part of new and broader CPNI rules. *See* Letter from Donna Epps, Vice President, Verizon, to Marlene H. Dortch, Secretary, FCC (Dec. 22, 2006). If the

(1) carriers may not release call detail records over the telephone unless the customer provides a password; (2) carriers may not permit customers to establish an online account using only the customer's account number or biographical data; and (3) carriers must notify customers of changes to billing address, establishment of new online accounts, and changes to passwords.

I. Implementing a Password Requirement for Call Detail Records

To implement the first of these safeguards (*i.e.*, the requirement that Verizon not provide call detail records over the telephone unless a customer provides a password), Verizon would have to re-train its 10,000 customer representatives and inform customers of the change. Verizon may also need to complete critical IT systems development work. First, in terms of training, Verizon would have to accomplish the following tasks as quickly as possible, which, as a practical matter, would take at least six months.

1. A new CPNI rule imposing this new password requirement would first have to be converted into Verizon training documents. This development and review process will take at least three to four weeks from when the Commission releases the Order.

2. After the training documents are finalized, Verizon must train the managers who will in turn train Verizon's 10,000 customer service representatives. Verizon typically conducts three to four "Train the Trainer" sessions to ensure that all managers have been educated about the new rule and know how to present them to the representatives. These sessions take two weeks and are scheduled two weeks prior to the actual face-to-face training of the representatives.

3. Approximately 10,000 customer representatives must then be trained. In order to continue to provide quality service to our customers while we are training our representatives, an expedited training program could require use of overtime. The training of 10,000 representatives on an expedited basis will take at least eight to twelve weeks – and perhaps longer depending on the final training schedule.

In sum, from the date of issuance of any Commission order to completion of expedited training for all 10,000 Verizon customer service representatives, the total training time is at least six months.

Commission does adopt rules that contain requirements different from these assumptions, the implementation timeline will be different. Verizon previously explained that, assuming that the Commission's order required carriers to make certain specified changes, Verizon would need 12-18 months to implement those changes. *Id*. This *ex parte* discusses a different set of proposed Commission requirements.

Second, customers must be informed about this change in federal rules and Verizon's business practices. Verizon must first develop a bill insert, but this process cannot begin until the Commission order is released. If the Commission order is released before early March, and the bill insert is also developed and approved before early March, Verizon would attempt to insert the notice of the change with the April billing cycle. Because customers are not all billed on the same day of the month, it will take a full billing cycle of 30 days for all customers to receive the bill insert. This means that, at the earliest, it would be May before Verizon could say with confidence that all Verizon customers had been notified of any change in FCC rules or Verizon's practices.

In addition, Verizon may decide that an effective way to implement the password requirement for call detail records over the telephone will require additional IT work. For example, Verizon may conclude that when a service representative pulls up a customer's call detail records, the representative should see a "pop-up" screen reminding him or her to ask for a password. In addition, Verizon may decide that it should add a standardized, dedicated "password" field to the various graphic user interfaces that the customer service representatives access when reviewing an account. Currently, some Verizon customers have passwords on their accounts, but those passwords cover general account access, and they are stored in different locations in the several billing systems in use across Verizon's footprint. Changes such as these will take at least six months.

In sum, in order to implement a new requirement that carriers not provide call detail records over the telephone unless a customer provides a password, it will take Verizon at least six months to train its 10,000 customer representatives, inform customers of the change, and complete critical IT systems development work.

II. Implementing Changes to Online Account Access and Customer Notice Procedures

To implement the other changes listed above, Verizon would need to perform the necessary IT systems modifications, software development and programming, and field testing before changes may be implemented across the Verizon footprint for our 32 million residential landline customers and 12 million online accounts as well as providing additional training to our employees. These tasks include:

1. In order to implement a requirement that Verizon change its authentication procedures before a customer can establish a new online account, Verizon may have to redesign its systems to validate a customer's identity based on information other than account code or biographical data. At a minimum, Verizon would likely have to create systems to generate random PINs, develop and mail letters to millions of customers with the PIN and logon information, and hire more Verizon customer service representatives to handle calls from frustrated and confused customers. Verizon would also have to set up a method and system to assist customers who lose their letters and/or forget their PINs.

It is important to note that Verizon's current practice of authenticating customers using a customer's account code is just as secure as authenticating using a Verizon-generated PIN. That is because the customer account code is contained on the customer bill and is therefore mailed to the billing address, just as any PIN would be. If the billing address is considered secure for the purposes of mailing a PIN, any information mailed to that address should also be considered secure.

Implementing a PIN requirement for online account set up would have other significant consequences. It would affect the ability of Verizon customers to place online orders for new Verizon features and services. Verizon's online ordering processes require existing customers to establish online accounts on Verizon.com when ordering certain Verizon services online, such as local, regional, or long distance calling plans. This is because when an existing customer wants to add a new feature or service such as a Verizon calling plan, the customer uses the "shopping cart" function that is accessible from the customer's "My Account" webpage, which also contains call detail records and other CPNI. In order to access the "My Account" webpage, the customer must first set up an online account and select a user name and password. If customers also needed a PIN to order new services such as calling plans, they would have to contact Verizon, ask for a PIN, wait for the PIN to be mailed and arrive, and then complete the online ordering/online account set up process. Requiring customers to obtain a PIN before they could set up an online account in order to order new features or services would frustrate customers, delay sales, and impede Verizon's ability to communicate with its customers. There is even less reason to require customers to have a PIN to establish an online account because it is highly unlikely that a pretexter would go to the trouble of ordering new services for a customer.

2. In order to establish a system that would notify customers every time there is a change to a password or billing address, or when a new online account is established, Verizon would have to change the numerous applications that house such information so that any change would trigger a centralized application to send notice to one of Verizon's mail/print distribution centers, that would in turn generate a letter for mailing to the customer. Verizon would have to overlay such a system with a check and review function so that Verizon could confirm that a triggering event occurred and that a letter was mailed. In addition, in order to handle returned mail, which in our experience usually represents about four percent of a typical Verizon mailing, Verizon may have to hire and train additional employees, which could also add to the amount of time Verizon would need to comply.

In sum, it will take Verizon at least six months to perform the essential IT systems modifications, software development and programming, and field testing, based on our current general understanding about the rules the Commission may impose. But if the Commission's rules are different from these assumptions or if the details of the order require additional IT systems work, the implementation timeline will be different.

III. Consistency with Commission Precedent on Implementation Periods

Providing a reasonable implementation period to make changes to carriers' internal CPNI procedures is consistent with Commission precedent in connection with CPNI rules and in other orders.

In the Commission's February 1998 CPNI Order, the FCC stated that its rules would become effective, and most would be enforceable, 30 days after Federal Register publication *Second CPNI Order*, 13 FCC Rcd. 8061, ¶ 202 (rel. Feb. 26, 1998). But the Commission deferred enforcement of the "flagging"[3] and "audit trail"[4] rules until eight months after the Order became effective because carriers needed to "conform their data systems and operations." *Id*. ¶ 202. Federal Register publication occurred on April 24, 1998, and the rules became effective 30 days later, on May 26, 1998. Consequently, enforcement of the flagging and audit trail requirements should have started on January 26, 1999.

On September 24, 1998, however, the Commission announced that it would postpone the enforcement of the flagging and audit trail rules that were scheduled to begin in January 1999 until six months after the Commission released an Order on Reconsideration addressing these rules, *Stay Order*, 13 FCC Rcd. 19390, ¶ 6 (rel. Sept. 24, 1998), which theCommission released in August 1999. *Order on Reconsideration*, FCC 99-223 (rel. Sept. 3, 1999). In the *Reconsideration Order*, the Commission decided that it would not pursue enforcement actions relating to the flagging and audit trail rules

---

[3] The 1998 flagging rules required that "carriers develop and implement software systems that "flag" customer service records in connection with CPNI . . . The flag must be conspicuously displayed within a box or comment field within the first few lines of the first computer screen. The flag must indicate whether the customer has approved the marketing use of his or her CPNI, and reference the existing service subscription . . . These requirements represent minimum guidelines that we believe most carriers can readily implement and that are not overly burdensome." *Id*. at ¶ 198.

[4] The 1998 audit trail rules required "that carriers maintain an electronic audit mechanism that tracks access to customer accounts. The system must be capable of recording whenever customer records are opened, by whom, and for what purpose . . . Such access documentation will not be overly burdensome because many carriers maintain such capabilities to track employee use of company resources for a variety of business purposes unrelated to CPNI compliance, such as to document the volume of computer and database use, as well as for personnel disciplinary matters. We further require that carriers maintain such contact histories for a period of at least one year to ensure a sufficient evidentiary record for CPNI compliance and verification purposes." *Id*. at ¶ 199.

until eight months after the *Order on Reconsideration*'s release, instead of the six month extension called for in the September 1998 *Stay Order*. *Id*. ¶ 119. The Commission explained that the additional two month extension would be "in the public interest." *Id*.

As this history of the flagging and audit trail requirements shows, the Commission has previously recognized that changes to carriers' internal CPNI practices and procedures can take many months and can be more difficult that initially expected. The changes of the sort under consideration now will be as difficult to implement. Therefore, the Commission should give carriers adequate time to make all necessary changes of the sort discussed in this *ex parte* letter and avoid the possibility of having to extend any deadline in the future.

This is consistent with Commission practice in other areas as well. Outside the context of CPNI, the Commission has also recognized the importance of reasonable implementation periods. *See, e.g*., *Review of the Emergency Alert System Order*, ¶ 56 (2005) (adopting an 18 month implementation plan for DBS providers to comply with Emergency Alert System rules); *Closed Captioning and Video Description of Video Programming Order*, 13 FCC Rcd 3272, ¶ 12 (1997) (adopting an 8-10 year phased approach for full captioning of video programming); *Telephone Number Portability Order*, 12 FCC Rcd 7236, ¶¶ 78-80 (1997) (establishing a 6-12 month window for Phase I implementation of number portability); *Enhanced 911 Order*, 11 FCC Rcd 18676, ¶¶ 63, 67-69 (1996) (adopting a 12-18 month implementation plan for E911).

* * * * *

In sum, the implementation period for any new CPNI rules of the sort discussed in this *ex parte* would take at least six months. An implementation period that is too short would create significant confusion and frustration for customers, and it would be impossible for carriers to comply with.

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

Respectfully submitted,