

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 14, 2006

Ex Parte

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
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:

Verizon and Verizon Wireless take the protection of customer confidential information seriously, and we are committed to guarding against the practice of pretexting. We support the Commission's goal of increasing the security of customer information by combatting pretexting. Our support includes cooperating with law enforcement, filing civil actions to uncover and stop otherwise anonymous pretexting operations, training our customer service personnel to detect and report conduct indicative of pretexting, and working with industry on safeguarding best practices. As we and other carriers have emphasized, the primary method to stop pretexting should lie in civil and criminal remedies against the pretexters. Indeed, Congress has just passed legislation addressing that precise issue, enacting tough new penalties against pretexters. *See Telephone Records and Privacy Protection Act of 2006, S. 2178/H.R. 4709, 109th Cong.* (as passed by Senate on Dec. 9, 2006, and by House on April 25, 2006). Verizon and Verizon Wireless publicly endorsed this legislation in January 2006 and worked closely with its sponsors to support its passage. With the legislation about to become law, the Commission should ensure that any action it takes advances the protection of customer information without hampering legitimate business between carriers and their customers, who are the victims of pretexting.

As Verizon and Verizon Wireless have stated, the Commission should establish a safe harbor for carriers that adopt and implement the new safeguarding practices. Our proposal is attached to this letter. To the extent that the Commission imposes new safeguarding requirements without a safe harbor, however, any new rules should be crafted so that they do not impose unnecessary burdens on the ability of customers to obtain information about their services or on the ability of carriers to provide it. Narrowly tailoring of any new safeguarding obligations is critical to avoid imposing unnecessary costs and burdens on the customers and carriers.

Any new Commission rules should reflect the following principles:

1. Carriers should have written procedures that are included with their annual certification, already required by the Commission's rules, summarizing the carriers' practices for protecting CPNI. Written procedures will help ensure that carriers and their employees are aware of and comply with specific safeguards for CPNI.
2. Carriers should make pass codes available to customers to place on their accounts and should inform customers that pass codes are available. But customers should not be forced to have a pass code in order to obtain most information about their account when they call a carrier's customer service department. Many customers would likely find it burdensome and inconvenient to establish and remember pass codes each time they call customer service. In addition, of the millions of customer calls that Verizon and Verizon Wireless receive each month, most seek information about the bill balance, minutes left on an account, calling plans, services, network coverage, or handset upgrades. None of this information is related to the pretexting issue. In addition, forcing customers to set up and recall pass codes for every call to a customer service center would impose substantial costs and burdens on carriers, who will likely have to hire additional employees to handle increased call volumes and "hold times." The significant burdens of this requirement on customers and carriers would far outweigh any incremental benefit in protecting against pretexting.
3. In light of the burdens on customers and carriers discussed above, pass codes should be required only when customers wish to access their online accounts or when they call their carriers' customer care centers to discuss call detail records over the telephone. A mandatory pass code requirement should not apply when a customer calls the carrier to question a specific call charge and provides the telephone number called (in the case of an outbound call) or the calling telephone number (in the case of an inbound call); the date of the call; and the approximate time of the call. It is important to note that carriers should not be *required* to provide any call detail records over the telephone -- some carriers may find it more effective simply to limit customer access to call detail records to an online account or a paper bill and not provide any call detail records over the telephone.
4. Carriers should notify customers if they determine that call detail records have been released to an unauthorized individual using fraudulent means, subject to carriers' obligations to comply with requests from law enforcement or otherwise in response to legal process.
5. Compliance with these requirements should constitute a "safe harbor" against enforcement. In 2003, in adopting its "do not call" rules for telemarketing, the Commission decided that a carrier that followed all of the specific safeguards set forth

December 14, 2006

Page 3

in the rules for preventing unlawful telemarketing, but nonetheless erroneously called a person on the do-not-call list, should not be penalized for doing so. *See* 47 C.F.R. § 64.1200(c). This approach is also appropriate where a carrier would not have willfully released CPNI to an unauthorized person. *See* 47 U.S.C. § 503(b). For example, an estranged spouse may well have access to all of the verification data needed to obtain call detail records, including a password. When a third party's fraud causes the release of CPNI despite the carrier's adherence to these reasonable safeguards, it would be unfair and unreasonable to penalize the carrier.

6. The Commission should exempt wireline business customers from these requirements because there is no evidence that pretexters are targeting these customers. Moreover, 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.

Verizon and Verizon Wireless are proposing the attached draft safeguarding regulations as one reasonable way to implement these principles. The companies may continue to refine these draft regulations because, as Verizon Wireless explained in its October 18, 2006 *ex parte* letter, there are "a variety of ways" that key safeguarding principles can be incorporated in new Commission policies or rules. The attached draft regulations are intended to replace the proposal in Verizon Wireless' October 18 *ex parte* submission.

Sincerely,

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

cc: Michelle Carey
Ian Dillner
John Hunter
John Branscome
Scott Bergmann

Section 64.2010 Protection of Call Detail Records for Customer Accounts

(a) *General Duty.* Carriers shall employ reasonable safeguards to protect customer call detail records in the carriers' possession, custody, or control against unauthorized disclosure to third parties. The rules set forth in this section apply only to residential wireline customers and wireless customers.

(b) *Reasonable Safeguards.* A carrier is eligible for the safe harbor set forth in section (d) below if it has implemented the following safeguards to protect against the unauthorized disclosure of call detail records of customer accounts:

(1) *Written Procedures.* The carrier has adopted and implemented written procedures to comply with this section to be followed by all employees, agents, and other persons with authority to access call detail records through the carrier. The carrier has included the written procedures with the certification required by Section 64.2009(e).

(2) *Use of Passcodes.*

(i) *Online Accounts.* If the carrier provides online access to call detail records, it first requires the presentation or entry of a unique pass code, a carrier-assigned customer code, or a comparably secure mechanism in order for a customer to establish such an online account.

(ii) *Customer Service Calls.* If the carrier provides access to call detail records through its customer service centers, it makes a unique pass code available for customers to place on their billing account and makes its customers aware of the availability of pass codes through bill inserts, on its web site, at point of sale, or by other means.

(iii) *No Separate Charge.* The carrier does not impose any fee or other charge for pass codes made available pursuant to this section.

(3) *Notification of New or Changed Pass Codes.* The carrier provides notification or confirmation no later than five business days after the establishment or change of a pass code on a billing account under this section using one of the following methods: (i) mail to the billing address on record for the customer; (ii) electronic mail to the electronic mail address on record for the customer; (iii) text message to the customer's handset; or (iv) telephone call placed to the telephone number designated on the account.

(4) *Online Access to Call Detail.* The carrier does not allow call detail records on a customer's account to be accessed through a carrier's online system, unless (i) the correct pass code or carrier-assigned customer code is provided; (ii) the correct answer to a challenge question previously set up on the account is provided; or (iii) the request is authenticated using a mechanism that is comparable to (i) or (ii) in its security.

(5) *Release of Call Detail Records Over the Telephone.*

(i) *Verification of the Caller.* To the extent that call detail records are available for the account and the carrier provides access to such records over the telephone during a call with the carrier's customer service center, and except as otherwise permitted below in (ii), the carrier discloses call detail records during a telephone conversation with an individual claiming to be the customer or an authorized party on the account only if: (A) the customer has previously established a pass code to protect such information; (B) the individual provides the pass code over the phone to the carrier; and (C) the carrier verifies that the pass code provided matches the pass code on the account.

(ii) *Verification of the Call.* Notwithstanding the above, a carrier that provides access to call detail records through its call centers may disclose information pertaining to a particular call, without verification of a pass code, if the individual requesting access to the information provides all of the following: (A) the telephone number called, in the case of an outbound call, or the calling telephone number, in the case of an inbound call; (B) the date of the call; and (C) the approximate time of the call.

(6) *Notification.* The carrier has written procedures in place to conduct a prompt investigation when the carrier has a reasonable basis to believe that an unauthorized person may have obtained call detail records by fraudulent means. The investigation includes, but is not limited to, a determination of the scope of the breach, identification of the breached records, and restoration of the integrity, security, and confidentiality of the applicable system or records. After the carrier has completed the investigation and determined that an unauthorized person has obtained a customer's call detail records, it has written procedures in place to notify the customer promptly. Customer notice may be delayed if a law enforcement agency determines that it would interfere with an investigation and requests a delay.

(c) *Call Detail Records.* As used in this section, "call detail records" means records of the originating telephone number for an inbound call to, or the destination telephone number for an outbound call from, the telephone number on the account.

(d) *Safe Harbor.* Any person or entity that discloses customer call detail records without authorization will not be liable for violating this section if it can demonstrate that the violation was inadvertent or the result of error and that, as part of its routine business practice, it employs the safeguards set forth in section (b) above.

(e) *Official Disclosure; When Disclosure Not Required.* Nothing in this section shall affect a carrier's rights and obligations with regard to furnishing call detail records to a law enforcement agency, an administrative agency, a court, or otherwise authorized by law, or otherwise affect exemptions authorized by law for permitting the use, disclosure, or access to CPNI without customer consent. Further, nothing in this section shall be

deemed to require a carrier to disclose call detail records over the phone or using an online system.