

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

March 13, 2007

Ex Parte

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th St., 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:

On March 8, 2007, Verizon filed an *ex parte* letter in this docket expressing Verizon's support for law enforcement's efforts to stop pretexting and pledging Verizon's assistance in ensuring that Verizon's CPNI practices do not hinder the legitimate needs of law enforcement. Verizon's March 8 letter also discussed Verizon's concerns about certain parts of the CPNI breach advance notification proposed by the Justice Department. *See* Letter from Paul J. McNulty, Deputy Attorney General, to Kevin J. Martin, Chairman, FCC, and accompanying attachment (Dec. 28, 2006).

Verizon is attaching an alternative CPNI breach notification rule that Verizon has shared with the Department.

Should you have any questions about this filing, please contact me at (202) 515-2527.

Respectfully submitted,

A handwritten signature in black ink that reads "Donna Epps".

Attachment

§ 64.2010 Notification to Law Enforcement of Breach.

(a) A telecommunications carrier having determined that a breach of its customers' CPNI has occurred shall notify law enforcement as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b).

(b) As soon as practicable, and in no event later than seven (7) business days, after determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigations (FBI) through a central reporting facility, and may contemporaneously notify any state or local law enforcement or consumer protection agency as permitted or required by state law. The Commission shall maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>.

- (1) Notwithstanding any state law to the contrary, neither the carrier nor any state agency shall notify customers or disclose the breach to the public until seven (7) business days have passed after notification to the USSS and FBI.
- (2) If the USSS or FBI determines that public disclosure or notice to customers would impede or compromise an ongoing potential criminal investigation or national security, such agency may direct the carrier or state agency not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier and any state agency when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security, and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and FBI pursuant to paragraph (b), and notifications made to customers. The record must include, if known, dates of discovery and notifications; a detailed description of the CPNI that was subject of the breach; and the circumstances of the breach. Carriers shall maintain the record for a minimum of two years. Nothing in this section shall be construed so as to require a record to be made public or otherwise disclosed in violation of attorney-client privilege, work product doctrine, or other protections for confidential, sensitive, or proprietary information.

(d) Definition. As used in this section, *breach* means access to a protected computer, as that term is defined in Section 1030 of Title 18, without authorization or exceeding authorized access, and thereby obtaining CPNI, where such access would require notice to a customer under any state or federal law; or the unlawful sale, transfer, or access to CPNI in violation of Section 1039 of Title 18.

(e) Nothing in this section shall prohibit a carrier from taking any corrective or other action to prevent further unauthorized access to CPNI.

(f) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.