

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 8, 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:

Verizon¹ has a long legacy of working cooperatively with law enforcement, and we recognize the government's valid interest in protecting ongoing investigations. Verizon will continue to work with law enforcement to provide as much assistance as possible to stop pretexting and to ensure that Verizon's CPNI practices do not hinder law enforcement's legitimate needs. Currently, for example, Verizon is providing assistance to the Federal Trade Commission in a civil complaint lodged in federal district court in Wyoming lawsuit against alleged databrokers. *See FTC v. Accusearch, Inc.*, No. 06CV0105-D (D. Wyo.).

Verizon has concerns about certain parts of the CPNI breach advance notification regulation proposed by the Department of Justice ("Department"). *See* Letter from Paul J. McNulty, Deputy Attorney General, to Kevin J. Martin, Chairman, FCC, and accompanying attachment (Dec. 28, 2006). Verizon has communicated these concerns directly to the Department. Many states have enacted statutory notice laws designed to address the same concerns, and these statutes provide useful insights on how the Commission could satisfy the legitimate needs of law enforcement and also address Verizon's concerns. Before enacting the Department's proposal, the Commission should address these concerns, or it should give parties additional time to file comments on how to revise the Department's proposed rules to address the concerns of both law enforcement and other parties, including industry.

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

First, the Department's proposal would require carriers to provide notice of all breaches of any size or scope to the government and would mandate that carriers delay notice at least seven business days to customers. *See* proposed rule § 64.2010(a). But carriers, including Verizon, already cooperate with law enforcement. Law enforcement may ask carriers to hold up notifying customers in certain for a month or more. But there is no reason to require delayed customer notification in all cases.

Second, the Department's proposed definition of "breach" is too broad and should be limited to those instances when a carrier has a reasonable belief that the conduct may violate the Telephone Records and Privacy Protection Act of 2006 or the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. *See id.* § 64.2010(d) (defining breach as "*any* unauthorized use, disclosure, or access to CPNI" (emphasis added)). Under the Department's proposed definition, purely internal systems glitches or unintentional employee access that resulted in immaterial access to CPNI would be considered breaches and would be subject to automatic notice to law enforcement and delayed customer notice. This is why the definition of breach should be tied to probable violations of federal law, which is consistent with the jurisdiction of the Secret Service and the FBI to investigate federal crimes. In addition, it would properly exclude instances in which the breach involving CPNI is non-material or unlikely to cause harm.

Existing state laws define "breach" to exclude breaches that are not material or when there is no expected harm to customers. Under Montana law, for example, "breach" means the "unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident." Mont. Code Ann. § 30-14-1704(4)(a) (Westlaw 2007). Similarly, under Kansas law, a "security breach" is "the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer." 2006 Kan. Sess. Laws 149 (tentatively codified at Kan. Stat. Ann. § 50-7a01(h)). *See also* Utah Code Ann. §§ 13-44-102, 13-44-202 (Westlaw 2007). Consistent with these state laws, any proposed federal definition of "breach" should carve out non-material and not harmful breaches and be limited to breaches involving CPNI that suggest or indicate criminal databrokering under the Telephone Records and Privacy Protection Act of 2006 or the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

Third, although the Department's proposed rule preempts state laws on customer notification, before imposing any of the Department's proposed rules, the Commission should determine if it has the authority to extend the preemption to all state customer notice requirements relating to the same incident. *See* proposed rule § 64.2010(a). If the Commission has such authority, a broader preemption is necessary to achieve the Department's objective because carriers could be caught between the competing demands of two sovereigns. For example, in many states, the obligation to notify customers applies not just to CPNI but to a broader category of "personal information," including financial information and Social Security Number. *See, e.g.,* Cal. Civil Code § 1798.82(e) (Westlaw 2007). As written, the Department's preemption provision would preempt notification laws only to the extent the breach involves CPNI. It would not

Ms. Marlene H. Dortch

March 8, 2007

Page 3

preempt state laws when the breach involves personally identifiable information that is not CPNI. As a result, under the Department's preemption provision, carriers would be required to delay customer notice as to CPNI but not as to the non-CPNI personally identifiable information, even when the same customers are involved, which could tip off targets and disrupt investigations.

Finally, the Department's proposal should be revised so that carriers have sufficient flexibility in the amount of information they are required to provide to law enforcement within seven days. *See* proposed rule § 64.2010(b). For some breaches, a carrier might know only basic information within seven business days, but, for others, carriers might have more information. For these reasons, the Department's proposal should be revised to give carriers sufficient flexibility in providing information to law enforcement to account for differences in the nature and scope of breaches involving CPNI.

In sum, Verizon supports the Department's legitimate interest in ensuring that customer notice does not hinder in any way the goals of law enforcement, but the Commission should address Verizon's concerns before enacting the regulations, or it should give all parties additional time to propose revisions that would meet the needs of law enforcement and other parties, including industry.

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.

cc: Michelle Carey
Ian Dillner
John Hunter
Scott Deutchman
Scott Bergmann
Tom Navin