



Office of the Deputy Attorney General

Washington, D.C. 20530

December 28, 2006

The Honorable Kevin J. Martin
Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: *In the Matter of Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information* (CC Docket No. 96-115); Request for Delayed Consumer Notification Concerning Breaches of Customer Proprietary Network Information ("CPNI")

Dear Chairman Martin:

I am writing to express the views of the Department of Justice ("DOJ") regarding the above-referenced Rulemaking regarding the privacy of Customer Proprietary Network Information ("CPNI"). Specifically, we request that the Federal Communications Commission (the "Commission"), in issuing any Rules requiring that carriers notify customers in the event of a breach of CPNI, include a mechanism allowing for delay of such notification at the request of law enforcement. Allowing for delayed consumer notification in appropriate cases enhances our ability to investigate the circumstances surrounding the loss of the data and, thereby, advances consumer protection.

As you are aware, DOJ has previously informed the Commission of its views on consumer notification of CPNI breaches.¹ We believe that prompt notice to law enforcement regarding security breaches is critical to the success of any investigation of those breaches. A

¹ See Comments of the United States Departments of Justice and Homeland Security, *In the Matter of Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, CC Docket No. 96-115 at 12-13 (filed Apr. 28, 2006).

Chairman Kevin J. Martin

Page 2

successful investigation can result in the apprehension of the wrong-doer before he has the opportunity to use stolen consumer information and can act as a deterrent to future breaches –ultimately protecting consumer interests.

We also strongly support the right of consumers to be notified in the event of breaches of personal data, including CPNI. However, immediate consumer notification of a breach may tip off the person(s) responsible, causing them, among other things, to destroy evidence, change their behavior, and accelerate their illegal use of any data before consumers or company victims can act. These concerns are particularly acute in cases involving access to electronically-stored records where the electronic evidentiary trail is often short lived and easily compromised by the target. Moreover, delayed notification may allow law enforcement to conduct an undercover investigation where, for example, the target returns to the breached system or is engaging in extortion or other ongoing criminal activity. Such an investigation, that could reveal further information regarding the scope of the breach, potential use of the data, or the involvement of other persons, would likely be curtailed if the target was aware that his activities had been discovered and that law enforcement was aware of the breach. Accordingly, the success of an investigation may depend on law enforcement's opportunity to delay such notification for a reasonable period.

The ability to conduct thorough and effective investigations of criminal data breaches is essential to promoting the security of CPNI and other data and protecting consumers from those who would misuse their personal information. For the foregoing reasons, DOJ requests that the Commission include in any Rules a mechanism allowing for delayed notification to consumers of CPNI breaches at the request of law enforcement. Enclosed is proposed language that would address these concerns and permit robust law enforcement investigations.

Sincerely,



Paul J. McNulty
Deputy Attorney General

Enclosure

§ 64.2010 Notification of Breach.

(a) A telecommunications carrier having knowledge of a breach of its customers' CPNI shall notify law enforcement and affected customers 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 reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>.

- (1) The carrier shall not notify customers or disclose the breach to the public until seven (7) full business days have passed after notification to the USSS and FBI, except as provided in paragraphs (2) and (3).
- (2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (1), in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
- (3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier 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 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 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 retain the record for a minimum of two years.

(d) Definition. As used in this section, *breach* means any unauthorized use, disclosure, or access to CPNI.