



U.S. Department of Justice

Criminal Division

*Computer Crime & Intellectual Property Section
1301 New York Ave., Suite 600
Washington, D.C. 20530
PHONE: (202) 514-1026
FAX: (202) 514-6113*

March 13, 2007

By ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street S.W.
Washington, D.C. 20554

Re: Notice of *Ex Parte* Presentation: *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)

Dear Secretary Dortch:

The United States Department of Justice ("DOJ"), together with the Federal Bureau of Investigation ("FBI"), participated today, March 13, 2007, in an *ex parte* telephone conversation with Commission staff regarding the above referenced matter. Deputy Assistant Attorney General Sigal Mandelker, Michael Stawasz, and Joseph Springsteen of DOJ's Criminal Division, together with Douglas Klein of the FBI, spoke with Tom Navin of the Commission. During the conversation, DOJ and FBI reiterated and elaborated on arguments made in their previous filings in this docket. In addition, DOJ and FBI provided a proposed rule (attached) that has been revised from the version provided in a December 28, 2006 letter from Deputy Attorney General Paul J. McNulty to Chairman Martin.

Sincerely,

/s/ Joseph E. Springsteen
Joseph E. Springsteen
Trial Attorney

cc: Tom Navin

§ 64.2010 Notification to Law Enforcement of Breach.

(a) A telecommunications carrier ~~having knowledge of a breach of its customers' CPNI~~ shall notify law enforcement ~~and affected customers of a breach of its customers' CPNI~~ 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) **Notwithstanding any state law to the contrary,** ~~t~~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) **Recordkeeping.** 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 available,** 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.~~ **As used in this section, a *breach* has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.**

(e) **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.**