August 8, 2007

VIA ELECTRONIC DELIVERY

The Honorable Kevin J. Martin
Chairman
Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 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 to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information (CC Docket No. 96-115) (WC Docket No. 04-36)*; Request for Clarification Regarding the Contents of Law Enforcement Notification Concerning Breaches of Customer Proprietary Network Information ("CPNI")**

Dear Chairman Martin:

CTIA-The Wireless Association® ("CTIA") writes to express its views regarding one aspect of the Report and Order and Further Notice of Proposed Rulemaking ("*CPNI Order*") released on April 2, 2007, by the Federal Communications Commission (the "Commission") in the above-referenced matter. As the Commission knows, CTIA worked closely with the U.S. Department of Justice (the "Department") in crafting the delayed notice proposal and supports the general proposition that law enforcement be notified in the event of a breach of security that results in the unauthorized disclosure of CPNI.[1] CTIA writes now to share its view that such reports to law enforcement need not and should not include CPNI and that records kept by carriers regarding a breach are not required to include the CPNI itself. The former would run afoul of various privacy protections whereas the latter is a security risk.

Reporting

The Commission required carriers to notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service and the Federal Bureau of Investigation. *CPNI*

[1] Letter from Christopher Guttman-McCabe, Vice President, Regulatory Affairs, CTIA – The Wireless Association® to Marlene Dortch, Secretary, Federal Communications Commission, CC Docket No. 96-115, filed February 5, 2007.

Order at ¶ 29. The Commission announced that it will maintain a link to the central reporting facility on its website at www.fcc.gov/eb/cpni. *Id*. at n.95. However, the Commission did not specify the form or content of such reports.

CTIA suggests that the Commission rely on a confidential[2] data entry form limited to the following:

1. Carrier name and TIN#
2. Point of Contact for Law Enforcement
3. Date the Carrier Reasonably Determined a Breach Occurred
4. Nature of Breach
    a. Computer Intrusion
    b. Physical theft or data loss
    c. Unauthorized Employee Access
    d. Pretexting
5. Description of CPNI (*e.g.*, *n* call detail records exposed)
6. Number of Customers Affected

CTIA understands that the Department shares CTIA's views. That is, the Department did not previously request, and it is not now seeking, to have carriers include actual CPNI in any security breach report.[3]

Moreover, the Commission should include an express prohibition on the submission of CPNI with any report to ensure the privacy and security of customer CPNI and to avoid running afoul of the Stored Communications Act ("SCA").[4] Section 2702 of the SCA prohibits a carrier from divulging transaction records to any governmental entity other than in accordance with the procedures specified in Section

---

[2] The Commission did not indicate whether such reports would be treated as confidential. CTIA assumes that the reports will not be public and will be protected from disclosure under the Commission's rules and law enforcement investigative exceptions under the Freedom of Information Act. To do otherwise would defeat the purpose of delayed notice if the reports themselves were public, and would expose the identity and contact information of carrier security personnel.

[3] Letter from Paul J. McNulty, Deputy Attorney General, United States Department of Justice, to Kevin J. Martin, Chairman, FCC, CC Docket No. 96-115 (filed Dec. 28, 2006).

[4] 18 U.S.C. §§ 2701 *et seq.*

2703 (*i.e.*, with appropriate legal process) or as otherwise permitted by law. *See* 18 U.S.C. §§ 2702(b)(5)&(8); 47 U.S.C. § 222(d)(2)&(4) (*e.g.*, to protect a carrier's rights or property or in an emergency).

Such a streamlined report will not diminish law enforcement's ability to "investigate and enforce illegal access to customer records."[5] The goal of the report should be to provide law enforcement with a rapid, timely notice so that prompt coordination with carrier personnel can commence. A more detailed report, or one that requires analysis of the legal ramifications of submitting CPNI along with a report, will only serve to delay reporting. While the Commission has permitted up to seven days after a determination of a breach to notify law enforcement, in cases appropriate for referral prior to the Commission's rule, CTIA's understanding is that law enforcement has been promptly informed.[6] A streamlined report will ensure the quickest notification possible.

Record-Keeping Requirements

The Commission also specified the following record-keeping requirements for any discovered breaches:

> [W]e require carriers to maintain a record of any discovered breaches, notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the USSS and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach. *Id*. at ¶ 29.

As with the report to law enforcement, CTIA believes that the record-keeping requirement does not include actually storing any CPNI separately or outside of the systems in place today. The "detailed statement of the CPNI breached" should, in essence, reflect the information reported through the Commission's Web site.

---

[5] Statement of Chairman Kevin J. Martin, Re: *Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Petition to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information (CC Docket No. 96-115 and WC Docket No. 04-36).*

[6] For example, when the breach occurs because of a theft of a computer that contains customer information from a retail store, local law enforcement often is notified immediately so that local pawn shops can be alerted and the investigation commenced while the trail is fresh. Computer intrusions generally are treated the same way, and the Commission no doubt knows that carriers are allowed to request law enforcement assist on premises during an attack in progress. 18 U.S.C. § 2511(2).

Conclusion

CTIA and its members are committed to maintaining the privacy and security of customer CPNI. By ensuring that reports to law enforcement and records of any breaches do not create the opportunity for further exposure, the Commission will further the goal of its *CPNI Order*. Pursuant to Section 1.1206 of the Commission's Rules, this letter is being electronically filed with your office. If you have any questions concerning this submission, please contact the undersigned.

Sincerely,

/s/ Christopher Guttman-McCabe

Christopher Guttman-McCabe

cc: Erika Olsen
Ian Dillner
Adam Kirschenbaum
William Dever
Marcus Maher