State of Florida

Public Service Commission

CAPITAL CIRCLE OFFICE CENTER • 2540 SHUMARD OAK BOULEVARD
TALLAHASSEE, FLORIDA 32399-0850

-M-E-M-O-R-A-N-D-U-M-

DATE: August 16, 2007

TO: Office of Commission Clerk (Cole)

FROM: Division of Competitive Markets & Enforcement (Moses)
Office of the General Counsel (Tan)

RE: Docket No. 060158-TL – Investigation of protection of customer proprietary network information by incumbent local exchange companies.

AGENDA: 08/28/07 – Regular Agenda – Proposed Agency Action – Interested Persons May Participate

COMMISSIONERS ASSIGNED: All Commissioners

PREHEARING OFFICER: Administrative

CRITICAL DATES: None

SPECIAL INSTRUCTIONS: None

FILE NAME AND LOCATION: S:\PSC\CMP\WP\060158.RCM.DOC

This is a recommendation to close the above-referenced docket as recent enactments of federal and state law effectively address unauthorized use or disclosure of Customer Proprietary Network Information (CPNI) and provide criminal punishment for violations.

Case Background

On February 22, 2006, staff opened this docket to investigate protection of CPNI by incumbent local exchange companies (ILECs). On March 27, 2006, the Florida Public Service Commission (FPSC or Commission) ordered the ILECs to review their current security measures for protecting CPNI information. During staff's investigation of CPNI data protection, Congress

passed the Telephone Records and Privacy Protection Act of 2006, making pretexting illegal.[1] The Federal Communications Commission (FCC) issued an order aimed at prevention and prosecution of CPNI violations. The Florida legislature also passed a law regarding CPNI, imposing criminal penalties and fines for CPNI violations.

Customer Proprietary Network Information

The Telecommunications Act of 1996 defines Customer Proprietary Network Information as "information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service" that the carrier possesses solely as a result of serving that customer. Customers' information, compiled from individuals' telephone calling behaviors, include subscribers personal data, services, amount of usage of services, and calling records.[2] A carrier is allowed to use individual calling records only for purposes such as increasing business or publishing directories, and prohibits a carrier from otherwise disclosing CPNI without express prior authorization by the subscriber.

Congressional Action

Last year Congress enacted a bill, HR 4709, the "Telephone Records and Privacy Protection Act of 2006". President Bush signed this bill regarding Customer Proprietary Network Information into law on January 12, 2007. The Act made it a criminal violation for knowingly and intentionally obtaining, or attempting to obtain CPNI by making false or fraudulent statements to an employee of a covered entity[3]; making such statements to customers; or providing a document knowing to be false or fraudulent; access customer accounts of a covered entity via the Internet or other conduct without prior authorization from the customer to whom the confidential records information related.

The law makes it unlawful to attempt to obtain, or cause to be disclosed to any person, customer proprietary network information (CPNI) relating to any other person by (1) making a false or fraudulent statement to an officer, employee, or agent of a telecommunications carrier; or (2) providing any document or other information to such officer, employee, or agent that the presenter knows or should have known to be forged, lost, stolen, or otherwise fraudulently obtained, or to contain a false or fraudulent statement or representation. Through the Federal Trade Commission, the law provides for enforcement. The solicitation of another person to fraudulently obtain CPNI and sale or disclosure of CPNI obtained under false pretenses are both prohibited. Violations are punishable by fine or imprisonment of up to 10 years.

The bill amended the Communications Act of 1934 to expand responsibilities of telecommunications carriers with respect to the confidentiality of subscriber (customer) calling records, both cellular and land-line based. The Federal Communications Commission (FCC) was

[1] Pretexting is a term used for someone that fraudulently represents themselves to the telephone company as the customer of whom they are trying to obtain telephone account information.
[2] Lists of dialed and received phone numbers are often called "calling records."
[3] "Covered entity" means a telecommunications carrier or a provider of IP-enabled voice service.

directed to prescribe regulations adopting more stringent security standards for CPNI (including detailed customer telephone records) to detect and prevent confidentiality violations.

Federal Communications Commission Rulemaking

The FCC issued an Order[4] on April 2, 2007, that requires telecommunications companies to increase protection of CPNI. This order supplements preexisting CPNI rules.[5] The order focuses on prevention and expanding the prosecution of unauthorized disclosure of CPNI, along with extending the pre-existing CPNI rules to providers of interconnected Voice–over-Internet-Protocol (VoIP) services. The rules are restrictive of use and disclosure without customer consent. The rules detail requirements to the carriers regarding the use, access to and disclosure of the records.

The carriers must obtain a customer's knowing consent before they use, disclose or give access to CPNI, unless the information is for the purpose of providing the already subscribed services. Previously, the FCC allowed for carriers to allow customers to "opt-out" and if the customer did not opt-out, CPNI could be used for marketing of non-subscribed services. Now the carriers must obtain express consent. Carriers must also authenticate calls prior to disclosing call records, keep details of CPNI use and disclosure records. The FCC also requests that carriers "take every reasonable precaution" to protect CPNI and urges carriers to go beyond the minimum requirements in the Order.[6] The FCC requires compliance with the new rules six months after the effective date of the Report and Order.[7]

The FCC rejected requests to preempt all state CPNI obligations.[8] The FCC further states that a carrier should petition the FCC for preemption if the carrier finds it difficult complying with both FCC requirements and a state requirement.

State Legislation

On July 1, 2006, Florida enacted a new law pertaining to CPNI.[9] The law, *Obtaining Telephone Calling Records by Fraudulent Means Prohibited*[10], specifically targets the telephone records obtained fraudulently from a telecommunications company.[11]

---

[4] *In re Implementation of the Telecommunication Act of 1996: Telecommunications Carrier' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report & Order and Further Notice of Proposed Rulemaking, (hereinafter "CPNI Report and Order") CC Docket No.96-115 and WC Docket No. 04-36, FCC 07-22 (rel. April 2,2007).

[5] *Second Report & Order and Further Notice of Proposed of Proposed Rulemaking*, 13 FCC Rcd 8061 (1998); 47 C.F.R. §64.2001-64.2009.

[6] *See*, CPNI Report and Order, 20, paragraph 32.

[7] The "effective date" is normally 30 days following publication in the Federal Register. The earliest effective date will be January 8, 2008.

[8] *See*, CPNI Report and Order at 33, paragraph 60. Additionally, the FCC found that they should allow states to also create rules.

[9] The state had already established authority over some CPNI issues under Section 364.24, Florida Statutes, which reiterates that illegal attempts to pass on CPNI is committing a misdemeanor of the second degree. The statute does

The law makes it a violation to obtain the calling record in a fraudulent manner or statement to customer, officer, employee or agent of a telecommunications company.of another person without the permission of that person. The knowing provision of fraudulently obtained information or provision of counterfeit information to a telecommunications company is also prohibited. It is also unlawful to ask another person to fraudulently obtain calling records from a telecommunications company or to sell or offer such fraudulently obtained calling records.

The law does provide law enforcement the ability to use records in the official course of business but does not exempt private investigators. The law allows the telecommunications companies access to their own records in the course of business.[12]

First-time offenders in violation of this law receive a first degree misdemeanor charge, punishable up to a year imprisonment and up to a $1,000.00 fine. Second or subsequent violation carries the charge of felony in the 3rd degree, punishable up to 5 years imprisonment and up to a $5,000 fine.

Federal statutes, the FCC order and state law address the issue of Customer Proprietary Network Information. The Commission is authorized to implement procedures consistent with the Act pursuant to Section 120.80(13)(e), Florida Statutes. Accordingly, the Commission has the implicit jurisdiction to protect consumers' information and to ensure that telecommunications companies are taking the proper measures to safeguard that information.[13] The Commission is vested with authority under Sections 364.01 and 364.24, Florida Statutes.

---

not preclude publicly available information nor does it preclude a telecommunications company from allowing its own customers from accessing their own customer account record.

[10] Section 817.484, Florida Statutes

[11] "Telecommunications company" has the same meaning as in Section 364.02, F.S. except that the term includes VoIP service and commercial mobile radio service providers. Section 817.484(1)(d), Florida Statutes.

[12] Additionally, companies may obtain records during testing of security procedures, investigation of allegations of internal misconduct, and recovery of calling records that were obtained or received by another person in a manner as defined by Section 817.484(2), Florida Statutes.

[13] Order Number PSC-06-0258-PAA-TL in the instant docket.

Discussion of Issues

Issue 1: Should this docket be closed?

Recommendation: Yes, this docket should be closed because recent enactments of federal and state law effectively address unauthorized use or disclosure of Customer Proprietary Network Information and provides criminal punishment. (Tan)

Staff Analysis: Yes, this docket should be closed because recent enactments of federal and state law effectively address unauthorized use or disclosure of Customer Proprietary Network Information and provides criminal punishment. Consequently, staff believes Commission action is no longer required or necessary in this matter.