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: February 23, 2006

TO: Director, Division of the Commission Clerk & Administrative Services (Bayó)

FROM: Division of Competitive Markets & Enforcement (Moses)
Office of General Counsel (Scott) KS RBS

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

AGENDA: 03/07/06 – Regular Agenda – Proposed Agency Action - Interested Persons May Participate

COMMISSIONERS ASSIGNED: All

PREHEARING OFFICER:

CRITICAL DATES: None

SPECIAL INSTRUCTIONS: None

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

Case Background

Recently there was a flurry of media stories about cellular call detail information being sold via the Internet. These websites also offer wireline telephone call detail records for long distance service and unlisted numbers. Telecommunications companies that provide local, long distance, and wireless services collect Customer Proprietary Network Information (CPNI) based on individuals' telephone calling behaviors. CPNI includes subscribers' names, addresses, services, amount of usage of services, and calling records. "Calling records" are lists of phone numbers that the subscriber receives calls from or dials. The ability to obtain unlisted telephone numbers is also advertised on some of the websites which could cause law enforcement officers' numbers becoming available, thus, endangering their lives.

It appears that the Internet website companies that offer these services are obtaining CPNI from the telephone companies using a method called "Social Engineering" or "Pretexting." 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. For example, a person calls the Incumbent Local Exchange Company (ILEC) and says that he thinks his long distance service has been changed without authorization and asks the ILEC to verify the long distance company to which his line is currently subscribed. With this information, the pretexter can then contact the long distance company and continue pursuing the long distance billing records.

Staff has been able to identify 40 websites that offer CPNI for sale. These companies are advertising this ability online and staff assumes that there are many additional companies that do not advertise, but have the same ability. With this many websites, it suggests that the security and identification requirements ILECs use to validate the identity of the CPNI requestor is insufficient to prevent unauthorized third parties from acquiring CPNI.

Staff conducted an investigation by ordering the long distance call detail records of a staff member's home telephone number and within a few hours, the information was provided. This information was provided to the Attorney General's office which filed a lawsuit against the two men that own the Florida based company.

Staff met with the representatives of the three largest ILECs to discuss the protection of CPNI which is protected by law pursuant to Section 222, of the Federal Telecommunications Act of 1996, and Section 364.24, Florida Statutes.

Staff requested the three ILECs to investigate the magnitude of the problem, identify how the information is being obtained, and what corrective action the companies plan to implement to prevent future disclosure of the CPNI. The companies filed their responses confidentially.

The Electronic Privacy Information Center petitioned the FCC on August 30, 2005, requesting that the FCC initiate rulemaking to require further implementation of security measures by the telephone companies to protect CPNI. The leaders of the House Energy and Commerce Committee have asked the FCC for all filings regarding CPNI with the FCC by the five largest wireless and wireline carriers, as well as details on when it plans to act on a petition filed by the Electronic Privacy Information Center. Rep. Joe Barton (R., Texas), the committee's chairman, has announced plans to introduce legislation to combat the problem.

The Florida Attorney General's office, as previously mentioned, filed a lawsuit against the two individuals that own the Florida based company that offers phone records for sale on the Internet. Sen. Aronberg (D-Green Acres) has introduced SB 1488 Relating to Telephone Calling Records; prohibits a person from obtaining or attempting to obtain calling records of another person by making false or fraudulent statements or by providing false or fraudulent documents to a telecommunications company, or by selling or offering to sell calling records that were obtained in a fraudulent manner; provides that it is a first-degree misdemeanor to commit first violation and a third-degree felony to commit second or subsequent violation.

The Commission is vested with authority under Section 364.24, Florida Statutes.

Discussion of Issues

Issue 1: Should the Commission order the ILECs to implement additional measures to secure CPNI information and provide a report by May 1, 2006, to staff containing a description of the additional security measures and the date the measures were implemented?

Recommendation: Yes. (Moses)

Staff Analysis: The ability to purchase call detail records for both wireline and wireless telephone numbers has been advertised on over 40 websites. Some websites also advertise the ability to provide unlisted telephone numbers based on a person's name or address. Staff began investigating the availability of these records for wireline service by placing an order on www.peoplesearchamerica.com on December 29, 2005 for the long distance call records of a Commission employee. Within hours staff received an accurate call detail record of the long distance calls that were pending being directly billed by the long distance company to the employee. The employee verified the accuracy of the call detail.

Staff verified that a person did contact Sprint on December 29 using the name of the staff employee in order to obtain pertinent information about the account. This method is called "pretexting" as described in the case background.

Staff met with Sprint, Verizon, and BellSouth on January 12, 2006, to discuss what procedures the companies use to secure CPNI and asked what additional security measures the companies could implement. The companies filed confidential responses which staff reviewed. Verizon appeared to have the most comprehensive approach to securing CPNI. Although the measures described in the responses may improve the security, staff believes further measures are necessary. Staff inquired again of the three companies on February 3, 2006, whether any additional measures other than those already described in the confidential filings had been implemented. The companies responded that no other measures have been implemented.

Staff completed additional testing to determine if call records could be obtained from other websites. Staff tested locatecell.com which provided erroneous records, and discreetresearch.com which did not produce records. Staff was successful on February 9, 2006, in obtaining call detail records using gum-shoes.com which resulted in accurate long distance call detail information being obtained. The ILEC, as well as long distance provider serving that customer is BellSouth.

The sale of CPNI has brought considerable attention from various agencies including the Federal Bureau of Investigation, the Federal Communications Commission, and the Federal Trade Commission. In addition, Attorneys General across the nation, including Florida, have been involved in legal actions against the Internet website companies. With this much attention, it is not unusual to see the problem disappear until the legal action and media attention subsides. Several state legislatures are also considering legislation to make the sale of CPNI illegal. All of this action is designed to eliminate the sale of CPNI, but the ultimate responsibility of securing the information lies with the telephone companies.

Staff believes strict measures should be implemented by the telephone companies to secure CPNI. Staff will continue to test websites and if staff is able to obtain CPNI through these websites, staff will bring a recommendation to the Commission at the appropriate time recommending the Commission impose penalties against the telephone company providing the information.

Legal Analysis

Jurisdiction

The Legislature's intent is clear in Section 364.01(2), Florida Statutes, that the Commission has the "exclusive jurisdiction in all matters set forth in" Chapter 364, Florida Statutes. Staff believes that 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 under §364.01 and 364.24, Florida Statutes. Section 364.01(4)(c), Florida Statutes, mandates that the Commission use its exclusive jurisdiction to "[p]rotect the public health, safety, and welfare by ensuring that monopoly services provided by telecommunications companies continue to be subject to effective price, rate, and *service* regulation." (emphasis added) Furthermore, Section 364.24(2), Florida Statutes, is within the Commission's purview and specifically provides that "[a]ny officer or person in the employ of any telecommunications company shall not intentionally disclose customer account records except as authorized by the customer [...]." Persons who violate this statutory provision commit a second degree misdemeanor and may be subjected to criminal punishment or fines under §775.082 or 775.083, Florida Statutes.

At the federal level, §222(a) of the Telecommunications Act of 1996 (Act) provides that all telecommunications companies have the duty to protect the privacy of their customers' proprietary information. Specifically, §222(c)(1) provides that

> "a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories."

The Commission has an implicit regulatory obligation to monitor the way in which telecommunications companies handle their customers' proprietary information. The Commission is authorized to implement procedures consistent with the Act pursuant to §120.80(13)(e), Florida Statutes. Staff believes that the Commission has the authority to require telecommunications companies to implement the appropriate safeguards to protect their customers' proprietary information.

Accordingly, staff recommends that the Commission order the ILECs to implement additional measures to secure CPNI information and provide a report by May 1, 2006, to staff containing a description of the additional security measures and the date the measures were implemented.

Issue 2: Should this docket be closed?

Recommendation: This docket should remain open pending the receipt of reports from the ILECs on progress of implementing additional CPNI security measures. Staff will continue to test various websites to determine if the security measures are successful. If staff determines the security measures are adequate, this docket should be closed administratively. (Scott)

Staff Analysis: This docket should remain open pending the receipt of reports from the ILECs on progress of implementing additional CPNI security measures. Staff will continue to test various websites to determine if the security measures are successful. If staff determines the security measures are adequate, this docket should be closed administratively.