



Leigh A. Hyer
Vice President-General Counsel, Southeast Region
Legal Department

ORIGINAL

FLTC07
201 North Franklin Street (33602)
Post Office Box 110
Tampa, Florida 33601-0110

Phone 813 483-1256
Fax 813 204-8870
leigh.a.hyer@verizon.com

May 1, 2006

Ms. Blanca S. Bayo, Director
Division of the Commission Clerk
and Administrative Services
Florida Public Service Commission
Capital Circle Office Center
2540 Shumard Oak Boulevard
Tallahassee, Florida 32399-0850

RECEIVED-FPSC
MAY - 1 PM 4:33
COMMISSION
CLERK

Re: DOCKET NO. 060158 -TL

Investigation of protection of customer proprietary network information by incumbent local exchange companies

Dear Ms. Bayo:

Pursuant to Commission Order PSC-06-0258-PAA-TL, Verizon Florida Inc. (Verizon) has reviewed its current security measures for customer proprietary network information and hereby submits its findings.

CMP

COM

CTR

ECR

GCL

OPC

RCA

SCR

Verizon has attached its "Safeguarding Customer Information" Methods and Procedures and a copy of a Fraud Alert bulletin that was distributed to all employees. Verizon considers all of the information provided in this response to be proprietary and is claiming confidential treatment pursuant to Section 364.183(1), Florida Statutes and Rule 25-22.006(5), Florida Administrative Code. Verizon considers the information confidential because, if it were publicly available, it would reveal Verizon's internal processes and procedures and thus potentially aid unscrupulous data dealers in their attempts to gain unauthorized access to information through social engineering tactics. Verizon understands this information will be protected from public disclosure until returned to the Company.

SGA As stated in the January 19, 2006 response to staff's request for information, Verizon recognizes the importance of protecting its customers' privacy, and customer privacy is a

SEC RECEIVED & FILED
ICent records
Jim
FPSC-BUREAU OF RECORDS

Confidential:
03846-06, 03847-06

DOCUMENT NUMBER-DATE
03845 MAY-1 8
FPSC-COMMISSION CLERK

priority. Verizon continually reviews its processes and procedures to ensure compliance with state and federal rules and laws and to recognize changes in technology as well as the evolving tactics of criminals seeking access to customer account information. Also, all Verizon employees are instructed on their responsibility to safeguard customer information. This responsibility is outlined in the employee Code of Business Conduct, is reinforced in procedures and refresher training, and compliance is ensured through routine service quality observation.

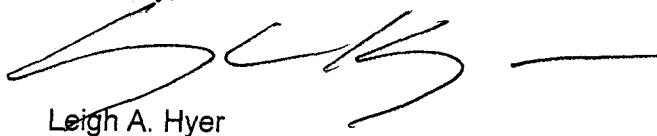
Employees are required to adhere to company policies and procedures, including adequately validating the identity of a caller prior to releasing specific information. Employees who violate company standards may be disciplined with sanctions up to and including dismissal. Verizon also has procedures in place for Verizon employees to verify the status of other purported employees before discussing account information (reference page 12 of the M&P).

Verizon's attached processes and procedures rely on information on the customer's bill from Verizon that is unique to that customer, and not available through other sources, to verify a customer's identity before providing any customer-specific account information. Verizon notified customers of this method of verification on a bill message appearing on their July 2005 bills (page 4 of the M&P). These procedures were developed in response to the recent rise in "social engineering" and were put in place throughout the Verizon footprint as recently as December 2005. Thus, these procedures represent a state-of-the-art solution that appropriately balances customer privacy with the customer's legitimate need to do business over the phone and Internet. Staff has also recognized the serious stance Verizon takes on this issue by noting that "Verizon appeared to have the most comprehensive approach to securing CPNI" in its recommendation for this docket.

At the March 7, 2006 Agenda Conference, the Office of the Attorney General proposed allowing customers to elect not to receive account information over the telephone or Internet. Verizon opposes this type of restriction, since it would have unintended consequences for the customer, interfering with the customer's ability to conduct business with Verizon and receive information in a timely manner that will permit the customer to make informed decisions regarding his or her service options. For example, if a customer called and asked about alternative services or package plans, Verizon's service representatives would be unable to answer the customer's basic service questions if the customer has elected not to receive account information over the phone. Therefore, customers would not be able to receive information about savings or the operational advantages of services that may be of interest to them. In order to make comparisons between existing packages and services, Verizon would need to pull the customer's records to discuss their current services and the potential effects (such as savings) of switching to another service or package. Questions regarding bill charges could not be answered, requiring the customer to provide their questions in writing. This practice would be overly burdensome and time consuming, especially for elderly and working customers. It also may cause such inconvenience to the customer that the customer will switch carriers rather than submit a request in writing (and wait several days for an answer). Under existing rules, a customer need not request a switch of its service provider in writing.

Therefore, Verizon has reexamined its methods to protect customer privacy and has determined that no additional measures are necessary. Verizon believes that its current security measures are as stringent as possible and will continue to strive for the highest standards to protect its customers.

Sincerely,

A handwritten signature in black ink, appearing to read 'L. Hyer', followed by a horizontal line.

Leigh A. Hyer

Enclosures

Verizon Florida Inc.

May 1, 2006

CONFIDENTIAL ATTACHMENT NO. 1

**Safeguarding Customer Information
Methods and Procedures**

**ENTIRE DOCUMENT, CONSISTING OF 15 PAGES,
IS CONFIDENTIAL**

Verizon Florida Inc.

May 1, 2006

CONFIDENTIAL ATTACHMENT NO. 2

**Verizon Employee Bulletin
Fraud Alert: Scammers Attempting to Gain Customer
Information**

**ENTIRE DOCUMENT, CONSISTING OF 1 PAGE,
IS CONFIDENTIAL**