Dulaney L. O'Roark III
Vice President & General Counsel, Southeast Region
Legal Department

5055 North Point Parkway
Alpharetta, Georgia 30022

Phone 678-259-1449
Fax 678-259-1589
de.oroark@verizon.com

REDACTED

February 19, 2008

Ann Cole, Commission Clerk
Florida Public Service Commission
2540 Shumard Oak Boulevard
Tallahassee, FL 32399-0850

080000-OT

Re: Staff Document Request 1-Review of Incumbent Local Exchange Carrier (ILEC) Data Security Programs

Dear Ms. Cole:

The enclosed documents are submitted in response to the above-referenced Staff Document Request. Please note that Verizon Florida LLC considers the highlighted portions of the response document and all of the documents submitted in response to Question 2.a. in their entirety to be proprietary and confidential business information and requests that they be treated confidentially pursuant to Section 364.183(1), Florida Statutes, and Rule 25-22.006, Florida Administrative Code. Also enclosed are two redacted copies of the confidential documents.

If there are any questions regarding this matter, please call me at (678) 259-1449.

Sincerely,

Dulaney L. O'Roark III

CMP 1
COM
CTR tas
ECR
GCL 1
OPC
RCA
SCR
SGA
SEC
OTH 1 cover records

Dulaney L. O'Roark III

Enclosures

c: David F. Rich

This claim of confidentiality was filed by or on behalf of a "telco" for Confidential DN 01301-08. The document is in locked storage pending advice on handling. To access the material, your name must be on the CASR. If undocketed, your division director must provide written permission before you can access it.

DOCUMENT NUMBER-DATE
01300 FEB 19 08
FPSC-COMMISSION CLERK

REDACTED

VERIZON FLORIDA LLC - RESPONSES

DOCUMENT REQUEST 1

(Review of Incumbent Local Exchange Carrier (ILEC) Data Security Programs)

Submitted to:

The Bureau of Performance Analysis

Instructions:

- Please provide with each answer to the questions below, the name and relevant contact information of the employee responsible so that, if necessary, that person can be contacted directly to elaborate, clarify, or provide additional information.
- If any responses involve information previously provided to Commission staff in the past six months, please cite the information or specific document, the name of the staff member to whom it was given, and the date on which the data was provided.
- Please label each response with a corresponding document request and item number (e.g., Document Request 1, Question 13).
- Please number all response pages.
- For purposes of this review the term "sensitive customer information" means social security, banking, or drivers license numbers, as well as customer address and phone numbers.

  It should be noted that the definition of customer sensitive information generally excludes name, phone number, and address since that is public information.

MANAGEMENT OVERSIGHT

1. **Please provide a current company organizational chart depicting work units, job positions and names of personnel responsible for administering customer information security.**

   Response:

REDACTED

2. **Please provide copies of:**

   Response:

REDACTED

a. **Company privacy policies relevant to customer data security and the protection of sensitive customer information.**

Response:

REDACTED

b. **Employee Code of Ethics for data security and the protection of sensitive customer information.**

Response:

REDACTED

c. **Company disciplinary policies and procedures which specifically address violations of customer data privacy and security protocols.**

Response:

REDACTED

3. **Please list all references to federal, state, or local rules, and regulations relating to customer data security with which the company must comply.**

Response:

REDACTED

4. **Please provide any data security industry best practices and standards to which the company adheres.**

Response:

REDACTED

1. **Payment Card Industry (PCI) Data Security Standard**

REDACTED

5. a. **Please identify the information collected from a new customer when opening an account.**

Response:

REDACTED

b. **Has management assessed the specific need(s) for and use of the personal information collected from customers? Please explain.**

Response:

REDACTED

6. **Please provide any risk analysis studies or evaluations performed by company management in the last 24 months that identified the adequacy of internal security controls relevant to sensitive customer information.**

Response:

REDACTED

INFORMATION TECHNOLOGY (IT) CONTROLS

7. **Does the company currently use full or partial masking of sensitive customer information? Please describe the masking methodologies employed.**

a. **Is such masking universal or selective across company network applications and software programs? Please explain.**

Response:

REDACTED

b. **How many employees currently have full (unmasked) access rights to sensitive customer information?**

Response:

REDACTED

8. **Please explain and describe what internal controls exist to ensure the proper handling and security of sensitive customer information.**

Response:

REDACTED

9. **Does the company employ a 'defense in depth' strategy for data security, using both intrusion detection systems (IDS) and intrusion prevention systems (IPS) to safeguard sensitive information? Please explain.**

Response:

REDACTED

10. **Please describe any changes or improvements made to the network data security protocols or access policies in the last 24 months.**

Response:

REDACTED

11. **Please describe and provide an example timeline for the processes associated with the receipt, validation and installation of security patches.**

Response:

REDACTED

12. **Does Information Technology:**

a. **Restrict employee access to customer information related software functions, data, and programs? Please explain.**

Response:

REDACTED

b. **Monitor and employee access to sensitive customer information? Please describe; explain protocols and procedures.**

Response:

REDACTED

c. **Produce regular management reports detailing employee access to sensitive customer information? If so, please provide an example of all such reports.**

Response:

REDACTED

13. **Please explain how risks specifically associated with Information Technology and relative to the release of sensitive customer information, are identified, evaluated, validated, isolated, prioritized, and corrected.**

Response:

REDACTED

14. **When establishing a new account, is a credit verification service (e.g. Experian) used?**

Response:

REDACTED

15. **Please describe the internal processes and timeline for changing employee access to sensitive customer information for those who terminate employment, retire, or transfer to positions which do not require such access.**

Response:

REDACTED

16. **Describe the virtual security safeguards and controls that are in place to protect the network and sensitive customer information for:**

a. **Remote employee access to the network remotely.**

Response:

REDACTED

b. **Offsite company facilities.**

Response:

REDACTED

USER AWARENESS AND TRAINING

17. a. **Please provide a copy of the policies and procedures used in collecting, safeguarding, storing, and destroying customer information.**

Response:

REDACTED

b. **Please provide company policies and procedures for processing customer payments (both electronic and paper transactions).**

Response:

REDACTED

18. a. **Please describe how the company conducts initial and recurrent training for employees relevant to data security policies, practices, and procedures.**

Response:

REDACTED

b. **Please provide a copy of current training materials relevant to security of sensitive customer information.**

Response:

REDACTED

OUTSOURCING CONTROLS

19. **Does the company allow authorized third parties to access its internal system infrastructure? If so, how is access to sensitive company and customer information protected from access by unauthorized third party employees?**

Response:

REDACTED

20. **Please provide the number of associates in subsidiaries and affiliated companies, or third party vendors, who have access to customers' full social security account number, banking information, address, date of birth, and/or driver's license number.**

Response:

REDACTED

21. **Please describe controls currently in place to prevent disclosure of customers' personal information by third party vendors.**

a. **What information security training do third party employees receive?**

Response:

REDACTED

b. **Does your company conduct background checks or require that background checks be conducted on third party employees?**

Response:

REDACTED

c. **Are third party employees with access to company sensitive customer information required to read and acknowledge the same privacy policies or Code of Ethics as company employees?**

Response:

REDACTED

AUDITING CONTROLS

22.

a. **Please provide a list of any internal audits, external audits, or external studies conducted by, or for, the company during the last 24 months regarding data security.**

b. **Please include the report date, title, a description of the scope and any findings, and the name(s) of the auditor(s).**

c. **Please provide a copy of any management responses to these audits.**

Response:

To be provided at a later date

23. **Please provide an incident description and explanation of remedial actions for security breaches from January 2006 through January 2008 for:**

    a. **Any sensitive customer information, including but not limited to credit card, bank account, driver's license, and social security account numbers.**

    Response:

REDACTED

    b. **Theft, loss, or compromise of company laptop computers or other portable storage devices such as storage disks, hard drives, pin drives, and personal data devices.**

    Response:

    Computer Equipment Loss/Theft

REDACTED

24. **How does the company internally assess the organization's information and customer data security practices? Please describe policies and procedures which govern such assessment, including the frequency, scope, and recommendation implementation.**

    Response:

REDACTED

25. **Are any internal or external audits planned in 2008 relevant to the security policies, practices, or procedures associated with protection of sensitive customer information? If so, please provide:**

    a. **Intent,**
    b. **Scope,**
    c. **Timeline, and**
    d. **Auditor(s)**

Response:

To be provided at a later date.

Corporate Policy Instruction

Policy No.: **CPI-810**
Issued: **November, 2001**
Subject: **Verizon Information Security Corporate Policy - Instruction**

REDACTED

ENTIRE DOCUMENT IS PROPRIETARY

Corporate Policy Instruction – Appendix A

Policy No.: **CPI-810 – Appendix A**
Issued: **November, 2001**
Subject: **Verizon Information Security Classification Schema**

REDACTED

ENTIRE DOCUMENT IS PROPRIETARY

Corporate Policy Instruction – Appendix B

Policy No.: **CPI-810 – Appendix B**
Issued: **November, 2001**
Subject: **Verizon Password Requirements and Responsibilities**

REDACTED

ENTIRE DOCUMENT IS PROPRIETARY

REDACTED

ENTIRE DOCUMENT IS PROPRIETARY

Corporate Policy Statement

Policy No.: **CPS-810**
Issued: **August 31, 2005**
Subject: **Information Security**

REDACTED

ENTIRE DOCUMENT IS PROPRIETARY

STATE OF FLORIDA

OFFICE OF COMMISSION CLERK
ANN COLE
COMMISSION CLERK
(850) 413-6770

Public Service Commission

ACKNOWLEDGEMENT

DATE: February19, 2008

TO: Verizon/O'Roark

FROM: Dorothy Menasco, Office of Commission Clerk

RE: Acknowledgement of Receipt of Confidential Filing

This will acknowledge receipt of a CONFIDENTIAL DOCUMENT filed in Docket Number 080000 **__ or, if filed in an undocketed matter, concerning** Response to staff's document request No. 1, review of ILEC data security programs, **and filed on behalf of** Verizon. **The document will be maintained in locked storage.**

If you have any questions regarding this document, please contact Marguerite Lockard, Deputy Clerk, at (850) 413-6770.