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

REDACTED

verizon

5055 North Point Parkway
Alpharetta, Georgia 30022

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

RECEIVED-FPSC
08 JUN 13 PM 4:15
COMMISSION CLERK

June 13, 2008

Ann Cole, Commission Clerk
Florida Public Service Commission
2450 Shumard Oak Boulevard
Tallahassee, FL 32399-0850

080000-07

RE: Staff's Draft Report – Customer Data Security of Florida Incumbent Local Exchange Carriers

Dear Ms. Cole:

The enclosed document is submitted in response to Staff's request that Verizon Florida LLC ("Verizon") review the claims of confidentiality it made in its June 5, 2008 filing in this matter. Please note that Verizon considers the highlighted portions of the enclosed draft report to be proprietary and confidential business information and requests that the information be treated confidentially pursuant to Section 364.183(1), Florida Statutes, and Rule 25-22.006, Florida Administrative Code. In addition, Verizon reaffirms that confidential treatment should be maintained for Verizon's responses to Staff's data request filed on February 19, 2008 and March 26, 2008 and that the entire set of Staff's work papers dealing with Verizon information be treated confidentially.

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

Sincerely,

Dulaney L. O'Roark DC

Dulaney L. O'Roark III

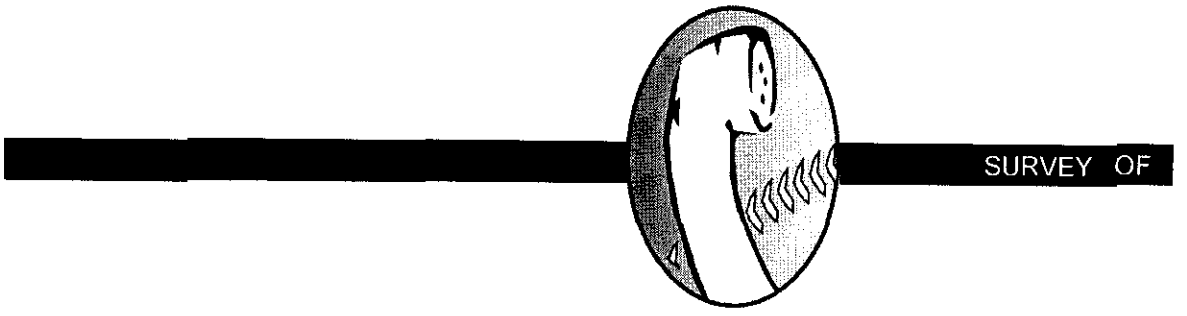
Enclosures

C Lisa Harvey
David Rich

This claim of confidentiality was filed by or on behalf of a "telco" for Confidential DN 05067-08. 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
05066 JUN 13 08
FPSC-COMMISSION CLERK

MAY 2008



Customer Data Security OF Florida Incumbent Local Exchange Carriers

By Authority of
The State of Florida
Public Service Commission
Division of Competitive Markets and Enforcement
Bureau of Performance Analysis

Review of

ILEC Customer Data Security

David F. Rich
Project Manager
Operations Review Specialist

Geoff Cryan
Regulatory Analyst II

May 2008

By Authority of
The State of Florida for
The Public Service Commission
Division of Competitive Markets and Enforcement
Bureau of Performance Analysis

PA-07-12-008

Table of Contents

7.0 APPENDICES

1.0 Executive Summary

1.1 Objectives

This review of Florida's three largest incumbent local exchange carriers (ILEC) was conducted on behalf of the Florida Public Service Commission (the Commission) by the Bureau of Performance Analysis. The objective of the review was to assess each company's policies, practices, and controls regarding the security of sensitive customer information.

The review's primary objectives were:

- To become familiar with, document, and evaluate each ILEC's policies, practices, and procedures for safeguarding sensitive customer data.
- To determine whether sufficient physical and virtual internal controls exist in each carrier to protect customer sensitive data and the network.
- To ensure that each company is in compliance with applicable state, federal, and industry guidelines regarding protection of sensitive customer information.

1.2 Scope

The review focused on examining each company's policies, practices, procedures, network systems, and operational controls for safeguarding sensitive customer data. Staff reviewed and assessed ILEC information technology (IT) security, key facilities' security, and customer account security in each company. Internal and external audits associated with IT and data security, from 2005 to the present, were also reviewed.

Specifically, staff focused its review on the following functional areas:

- Management Oversight
- Information Technology Controls
- User Awareness
- Outsourcing Controls
- Audits of Data Security

1.3 Methodology

Each ILEC was reviewed separately, but identical criteria were employed so that comparative assessment would be possible. During the review, staff gathered information from each company through document requests. After studying company responses, staff conducted

on-site visits with each company. Key company personnel in the functional areas under review were interviewed. This review was conducted between January and April 2008.

Each company's policies, practices, and procedures were compared to applicable state and federal statutes relevant to the protection of sensitive customer data. Physical and virtual security systems currently in use, other measures undergoing implementation, and security concepts in stages of either planning or development were reviewed.

To assess and compare each company's overall security posture, staff used information gathered from document reviews, on-site interviews, and facility visits to assess each company's overall security status. Areas of concern were discerned, as were best practices currently in use for these ILEC's.

1.4 Overall Opinion

None of the reviewed companies reported, or are aware of, any major breaches involving sensitive customer information in the previous two years, the period covered by this review. However, each company is variously impacted by the accelerated pace of evolving technology. While the safeguards for protecting sensitive customer data are continually improving, the technology used to breach such safeguards improves in parallel. Technological advances can render obsolete or ineffective those security measures initially considered to be comprehensive and of potentially long duration. It is a constant spiral of action and reaction.

"None of the reviewed companies reported, or are aware of, any major breaches involving sensitive customer information in the previous two years. . . ."

EXHIBIT 1 presents a summary of the data security issues observed during staff's review. Where staff found each category of controls to be appropriate and adequate, it is indicated by a solid circle (!). An issue is indicated by an open circle (").

The findings for each company are summarized on the following page. Additional discussion of staff's conclusions for each company is contained in chapters three through seven.

Two appendices are located at the back of this review. **APPENDIX A,** is a chart comparing ILEC customer data security practices. **APPENDIX B** provides details on the sensitive customer information each ILEC collects, its use, and whether this information is masked for security. Explanatory notes provide additional information.

Sensitive Customer Data Security Issue Summary

MANAGEMENT OVERSIGHT			
CONTROL ELEMENTS	AT&T	EMBARQ	VERIZON
Clearly understands that information security is a management responsibility			M
Personal information is collected			M
Assesses the appropriateness of the information collected from customers			M
Limits the use and disclosure of customer personal information			M
Controls for remote access exist			M
IT CONTROLS			
	AT&T	EMBARQ	VERIZON
Appropriate data security management function exists			M
Appropriate information security policies and procedures exist			M
Access to customer data is physically limited			M
Access to software, data, and functions are restricted			M
Changes to software programs are fully authorized, tested, and controlled			M
Management routinely monitors and assesses system security			M
USER AWARENESS			
	AT&T	EMBARQ	VERIZON
Adequate privacy and data security policy and procedures exist			O[1]
Proper training on privacy and data security policies is provided			M
Penalties for violations of privacy or data security policies are documented			M
OUTSOURCING CONTROLS			
	AT&T	EMBARQ	VERIZON
Controls are in place to prevent disclosure of customer information			M
AUDITING CONTROLS			
	AT&T	EMBARQ	VERIZON
Access to competent data security auditing resources exist			M
Data security is periodically accessed			M
IT breaches are reported to appropriate management			M

M **No Issue** O **Issue**

[1] Excessive intervals between Code of Conduct affirmations, out of date security policies and a lack of focused policy discussion for customer-specific sensitive data security. See section 5.3 for details.

1.4.1 AT&T

1.4.2 EMBARQ

1.4.3 VERIZON

Verizon has policies, practices, and procedures in place to protect sensitive customer information. Company management acknowledges its own overriding responsibility for information security while using multiple methods and media to instill a similar sense of individual responsibility in every employee. Virtual and physical security now in use are in keeping with the best industry practices, layered for a defense in depth, and appear to be effective.

Staff believes that Verizon's masking of social security numbers in all customer service applications is exemplary. So, too, is the interactive voice system which allows customers to set up credit or debit bill payment. This eliminates the need for customer service representatives to process any banking information and eliminates all risk of compromise to such data.

However, staff does have some concern about two items connected with Verizon policies relevant to sensitive customer information. These concerns center around two minor issues:

Written security policies do not contain appropriate emphasis on *customer* sensitive information security and some have not been updated for five years or more.

Employee Code of Conduct and business ethics affirmations are not regularly updated on a set schedule.

Most Verizon policies covering data security issues also do not provide a focused discussion about the protection of sensitive customer information. Instead, these policies demonstrate an orientation toward company privacy and the protection of Verizon proprietary information. Although the majority of privacy and data security policies currently in use do not specifically address the protection of sensitive customer information, Verizon management states that it believes existing materials help create an overall corporate attitude of awareness for safeguarding sensitive information. Staff believes Verizon should thoroughly review current

policies and procedures, determining whether they are specific and adequate for comprehensive protection of sensitive customer information.

Some written policies are old, and in the dynamic environment of modern technological change and cyber-security concerns, these may be of diminishing value or simply outdated. *CPI-810* series was published in 2001 and, so far as can be discerned, has never been updated. If this and other security-related policies and procedures have not undergone a thorough vetting since the early part of this decade, staff believes it would be wise to schedule such a review.

Staff believes that Verizon's policy of reaffirming employee acknowledgement of the Code of Conduct and business ethics only upon "significant change" is also inadequate. Verizon employees could only estimate that such changes and the corresponding reaffirmation occurs approximately every three years. Staff believes this an inordinately extended period of time between affirmations of a critical component to the security of sensitive customer information. Staff recommends that such reaffirmations occur at least biannually.

2.0 Background and Perspective

In general terms, identity theft is the use of someone's personal information with the intent to commit fraud. Identity theft can include the establishment of a new account without authorization, the misuse of an existing account and the establishment or misuse of government documents and benefits.

"The social security number is arguably the single most important item of information necessary to commit identity fraud."

The social security number is arguably the single most important item of information necessary to commit identity fraud. The function of the social security number has evolved greatly over time, from a simple tracking number initially used for the federal government retirement system to more of a personal identification number used by entities ranging from the Internal Revenue Service to banks, credit reporting agencies, and various service providers. This evolution of the social security number has created a need to more adequately protect and secure its use by the owner and exposure to those who might exploit it. While the social security number is the most critical component for identity theft, other information such as date of birth, a driver's license number, home address, phone number, bank account and routing information, and credit account numbers can also be useful in facilitating identity theft.

Individuals bear the ultimate responsibility to judiciously secure personal information. Many times, identity theft occurs when a victim loses personal information or carelessly exposes such information to opportunistic thieves. However, consumers must frequently entrust personal information to a business or agency. In doing so, there is a reasonable expectation that reputable companies will earnestly protect this sensitive information.

2.1 Identity Theft

Results of an FTC-sponsored survey on identity theft undertaken in 2003 highlighted several critical things. The threat of identity theft is credible, thefts are no longer isolated, and the problem is increasing. The report also pointed out that, more than ever before, adequately protecting customer sensitive information is vital for ensuring consumer confidence.

The *2006 FTC Identity Theft Survey Report* indicated that during 2005, 3.7 percent of the U. S. population experienced some type of identity theft. In the previous 5 years, 12.7 percent (approximately 27 million citizens) reported being victims of some type of identity theft. The report showed that identity theft impacted approximately 8.3 million American citizens during 2005, at an estimated average cost of $1,882 per victim. The estimate of total losses nationwide is $15.6 billion and the median of hours required by victims to resolve impact is ten hours. However, nearly one-third of complainants required 40 hours or more to resolve the issues.[2]

[2] *2006 FTC Identity Theft Survey Report,* published in November 2007

The FTC annually tracks identity theft complaints by type and location. In 2006, the latest data available, Florida ranked fifth in the nation with 98.3 cases per 100,000 population and a total of 17,780 reported victims. The Miami-Fort Lauderdale Metropolitan Statistical Area had the highest number of Florida complainants with 7,557.[3]

". . .Florida ranked fifth in the nation with 98.3 cases per 100,000 population and a total of 17,780 reported victims."

The problem of identity theft is growing in Florida. The reported number of victims within the state has steadily increased each year since 2002:

Year	Number of Victims
2002	12,816
2003	14,119
2004	16,062
2005	17,048
2006	17,780
2007	19,270

These numbers represent those victims who notified authorities of the crime; the actual total number may be significantly higher. In the last full year for which categorized data is currently available, the 2006 FTC study noted that 26 percent reported the crime to the FTC, state or local government, and local police. Thirty-six percent notified a credit agency.[4]

The Federal Trade Commission categorizes identity theft complaints based on how victims' information was misused, including telecommunications fraud. Of note, the 2006 Florida data indicates that 3.6 percent of complainants reported unauthorized establishment of new telecommunications accounts.[5]

2.2 Data Security Breaches

One of the most publicized breaches occurred in 2005, when the consumer data broker, ChoicePoint, Inc., admitted that it had compromised 163,000 consumers in its database. The company sold personal information, such as names, social security numbers, birth dates, employment information, and credit histories to an international group posing as legitimate American businessmen. The individuals lied about their credentials and used commercial domestic mail drops to receive the information. ChoicePoint not only ignored red flags, but used unsecured fax machines for correspondence.

Also in 2005, Bank of America admitted losing a back-up file containing personal information for up to 1.2 million customers. In the same year, Bank of America, Wachovia, Commerce Bancorp, and PNC Financial Services Group uncovered illegal sales by employees of

[3] Identity Theft Victim Complaint Data, Florida, January 1 – December 31, 2006, FTC, Washington, DC, Fig 4a
[4] *2006 FTC Identity Theft Survey Report, November 2007*
[5] Identity Theft Victim Complaint Data, Florida, January 1 – December 31, 2006, FTC, Washington, DC, Fig 2

sensitive customer information. Over 676,000 customers were affected by the internal breach in what was labeled at the time as potentially the "biggest security breach to hit the banking industry."[6]

2.2.1 Florida Breaches

Companies operating within Florida are not immune to unintentional exposure or intentional breaches of customer information. The following list highlights recent events in which customer information was exposed through unauthorized events:

- In March 2005, Customer records of a Florida-based subsidiary of the LexisNexis Groups were compromised when hackers used malicious programs to collect valid customer identification, passwords, and access the company's database. The hackers eventually gained access to 310,000 customer records.

  In February 2006, a contractor for Blue Cross and Blue Shield of Florida sent the names and social security numbers of current and former employees to his home computer. This was a clear violation of company policy. The former computer consultant was ordered to reimburse BCBS $580,000 for expenses related to the incident.

  In May 2006, hackers accessed the Vystar Credit Union in Jacksonville, FL. They collected the personal information of approximately 34,000 members, including names, social security numbers, date of birth, and mothers' maiden names.

- In April 2007, ChildNet, an organization that manages Broward County's child welfare system, had a laptop stolen by a former employee. The laptop contained social security numbers, financial and credit data, and driver's license information. Approximately 12,000 adoptive and foster-parents were adversely impacted.

  In June 2007, Jacksonville Federal Credit Union realized that social security and account numbers of 7,766 of its members were accidentally posted, unencrypted, onto the Internet. The search engine Google indexed these records within its search criteria, exposing them throughout the World Wide Web.

- In July 2007, Fidelity National Information Services, of St. Petersburg, reported that approximately 2,300,000 customer records were stolen by a worker from a subsidiary company. The information stolen included credit card information, bank account numbers, and other sensitive personal data.

  In November 2007, Memorial Blood Centers reported a discovered theft of a laptop computer holding donor information. About 268,000 donor records contained the donor's name and social security number. The laptop computer was stolen in downtown Minneapolis during preparations for a charity blood drive.

[6] *Bank Security Breach May Be Biggest Yet.* May 23, 2005. Retrieved July 2007. www.Money.cnn.com

- In December 2007 to March 2008, it was discovered that a breach of the computer system led to the theft of about 4.2 million credit and debit card numbers from the Hannaford and Sweetbay stores. Hannaford operates 165 stores in the Northeast and there are 106 Sweetbay supermarkets in Florida.

- In February 2008, an Information Security Analyst was sentenced to 50 months for aggravated identity theft and access device fraud. The individual had used an assumed online identity to sell approximately 637,000 stolen credit card numbers through a Web site frequented by individuals engaged in credit card fraud. Fortunately, the two biggest customers turned out to be undercover Secret Service agents.

- In April 2008, Lifeblood Mid-South reported a missing laptop. An internal investigation uncovered a second laptop missing from Lifeblood's primary blood supplier. Stored inside both computers were donor names, birth dates, and addresses. In the majority of cases, the social security number, driver's license and telephone numbers, e-mail address, ethnicity, marital status, blood type and cholesterol level were also compromised.

2.2.2 Potential of Exposure

Privacy Rights Clearinghouse, a nonprofit consumer information advocacy organization, annually compiles a listing of all data breaches involving sensitive customer data. In those incidents reported 2005 to the present, the majority of identity breaches can be categorized into four types:

- Technology
- Online Exposure
- Insiders
- Improper storage or disposal of customer records

Technology exposure can include unauthorized access into a company computer or server, especially those that store sensitive information in an unencrypted format. Also, this could include the unintentional or intentional downloading of malicious software to a company network not adequately secured with antivirus applications.

Online exposure can include personal information that is inadvertently loaded onto the internet. Search engines, such as Google, can be used to mine data from company websites and expose this information to a vast, worldwide audience through the internet. E-mails that include personal information may also be sent inadvertently to the incorrect addressee and unencrypted e-mails may be intercepted by hackers or malware.

Insiders can be dishonest employees with intent to commit fraud, or well-intentioned workers who commit a simple error in judgment. A dishonest employee may work for any corporation or agency. Employees with access to personal information may use extreme means to collect and steal personal information. Devices such as iPods, personal USB storage devices, and cell phones may provide a dishonest employee the means to collect, store, and transmit data.

Well intentioned, honest employees may also take sensitive customer information off-site for legitimate reasons but have the misfortune of a theft or loss while away from the office.

Improperly stored or disposed records containing sensitive customer information can be a tempting target for thieves. Improper storage can include unsecured paper files and unshredded or partially destroyed documents and electronic media. Mailings that include sensitive personal data can easily be stolen and lead to a breach of information. Improper destruction or disposal of old hardware can also lead to a security breach if memory devices are not properly purged.

2.3 Federal and State Authority

Several federal and state statutes or initiatives govern data security and identity theft. These apply either directly or indirectly to Florida's incumbent local exchange carriers and should be considered in developing security practices and procedures.

2.3.1 US Code, Title 47, Chapter 5, Subchapter II, Part I, §222; Privacy of Customer Proprietary Network Information

Under provisions of this statute, which went into effect in January 2006, telecommunications carriers have an obligation to protect the confidentiality of customer proprietary network information (CPNI). The statute defines CPNI as:

> Information relating to the quantity, technical configuration, type, destination, location, and amount of use of telecommunications services subscribed to by any customer, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.
>
> Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

Telecommunications carriers that either receive proprietary information directly from individual customers or from another carrier, for purposes of providing any telecommunications service, shall use the information only for this purpose and are prohibited from using the information for marketing or other purposes.

Except as required by law or with the approval of the customer, a carrier that receives or obtains customer proprietary network information by virtue of an offer to provide these services can only use, disclose, or allow access to CPNI in its provision of the service. Carriers are allowed to publish directories containing personal information such as name, address, and phone number. Customers may opt-out of such directories by choosing to have an unpublished number.

The statute also allows publication of aggregate data by telecommunications carriers. Such collective data relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

Sensitive customer information studied during this review falls outside the definition of CPNI as contained in this statute. This review concentrates on how Florida ILECs collect, use,

and safeguard such non-CPNI customer information social security and driver's license numbers, banking information, and credit card data.

2.3.2 Identity Theft and Assumption Deterrence Act 1998

In 1998, the Federal government enacted the Identity Theft and Assumption Deterrence Act. This measure made it a violation of federal law to intentionally misuse another person's identifying information or existing accounts, or to establish an account using his/her name.[7] The Act charged the Federal Trade Commission (FTC) as the principal federal governmental agency responsible to protect consumers from identity theft. Victims of identity theft can now report the crime to the FTC, which is responsible to collect complaints and then share the information with federal, state, and local law enforcement.

2.3.3 Fair and Accurate Credit Transaction Act 2003

This amendment to the Fair Credit Reporting Act is designed to help elevate attention given to preventing identity theft. Two components of the law require companies to truncate credit and debit card information on printed receipts, and to properly dispose of customer records. All credit card machines must be programmed to print only the last five-digits of the card information on a receipt, and may not include the expiration date.

Disposal requirements instruct businesses on methods to be used for documents containing customer information. Proper disposal includes burning or shredding of paper reports and completely erasing electronic storage devices. Such services can also be contracted to a qualified disposal company.

2.3.4 Fair Debt Collections Privacy Act

This act specifically limits the information that a creditor, or its agent, can provide to a third party. For instance, this legislation prevents a creditor, or the creditor's agent, from disclosing to a third party that an individual is in debt. This law also prevents a service provider from disclosing any past-due or charge-off information to anyone other than the customer of record or a previously designated, authorized user.

2.3.5 Presidential Task Force of Identification Theft

In May 2006, an Executive Order was issued establishing the President's Task Force on Identity Theft. This task force, headed by the Attorney General and the Chairman of the Federal Trade Commission, was charged to "craft a strategic plan aiming to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution."[8] The April 2007 final report featured a strategic plan recognizing that "No single federal law regulates comprehensively the private sector or governmental use, display, or disclosure of social security numbers; instead, there are a variety of laws governing social security number use in certain sectors or in specific situations."[9] The Task Force has recommended the development of a comprehensive record on private sector use

[7] Public Law 105-318,112 Stat.3007 (October 30,1998)
[8] The President's Identity Theft Task Force, Combating Identity Theft – A Strategic Plan, 2007, p. viii
[9] The President's Identity Theft Task Force, Combating Identity Theft – A Strategic Plan, 2007, p. 24

of social security numbers, including evaluating their necessity. The major policy recommendations from the Task Force are:

- Federal agencies should reduce the unnecessary use of social security numbers, the most valuable commodity for an identity thief.
- That national standards should be established to require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft.
- Federal agencies should implement a broad, sustained awareness campaign to educate consumers, the private sector, and the public sector on deterring, detecting, and defending against identity theft.
- A National Identity Theft Law Enforcement Center should be created to allow law enforcement agencies to coordinate their efforts and information more efficiently, and investigate and prosecute identity thieves more effectively. [10]

The Task Force believes that these changes are key to waging a more effective fight against identity theft and reduce its incidence and damage. Some recommendations can be implemented relatively quickly; others will take time and the sustained cooperation of government entities and the private sector.

2.3.6 Florida Statute 817.568 and 817.5681

Florida Statute 817.568 makes it a crime to fraudulently use another person's identifying information without first obtaining consent.

2.4 Florida Public Service Commission Role

Florida Public Service Commission ("the Commission") has limited specific jurisdiction regarding the security of sensitive customer data or its storage. However, within the existing framework of those measures, the Commission seeks to monitor the activities of regulated businesses, ensuring that adequate safeguards have been put into place to protect sensitive personal information from compromise. Chapter 350.117 of the Florida Statutes allows the Commission to conduct management and operation audits for any regulated company to ensure adequate operating controls exist. In accordance with that authority, this report addresses whether each ILEC audited for customer data security has adequate sensitive customer data controls in place. The audit particularly focused on management, information technology, user awareness, outsourcing, and auditing. The following company chapters address these controls in a question and answer format.

[10] The President's Identity Theft Task Force, Combating Identity Theft – A Strategic Plan, 2007, p. 4

5.0 Verizon

Verizon Florida provides landline service to approximately 1.3 million customers in the state. The company serves a 5,879 square mile footprint in Hillsborough, Pinellas, Pasco, Polk, Sarasota, and Manatee counties. Verizon Florida has [redacted] employees.

5.1 Management Oversight

Does Verizon management have a clear understanding that information security is a management responsibility?

Responses to staff inquiries demonstrate an acknowledgement by Verizon that information security, specifically sensitive customer information, is a clear and ongoing management responsibility. Management is responsible for establishing an appropriate corporate climate that elevates information security. They do this by approving appropriate policies, practices and procedures, allocating resources to information security concerns or programs. These establish an environment in which employees protect sensitive customer information.

Verizon management states that it recognizes that the best information security is only possible with coordination between all levels of the corporate hierarchy. Verizon states the corporate goal is to make employees fully capable of protecting sensitive customer information. Verizon stated that the company accomplishes this objective with an employee training program, management supervision of the workplace, mentoring and retraining of employees when necessary, and requiring periodic reaffirmation of the *Verizon Privacy Principles* statement.

What type of personal information does Verizon collect from customers?

When initiating a new account and performing credit checks as part of the process, Verizon customer service representatives (CSR) collect the items shown below using an application called the New Installation Wizard. The items collected to initiate basic service are:

Items required for the credit check are:

[redacted]

Has Verizon management assessed the appropriateness of the information collected from customers?

Verizon asserts that its management assesses the need for and the use of personal information collected from customers. The security risk associated with collection, retention, and destruction of sensitive customer information when no longer needed is also weighed. Management acknowledges its responsibility to assess risk associated with the appropriateness of the types of sensitive personal information collected from its Florida customers. Management has reviewed and approved the types of personal information currently collected. Additionally, the company stated that ongoing oversight and management of internal security controls have proven effective in mitigating risks to acceptable levels.

Comprehensive policies, practices, and procedures exist relating to the handling, collection, safeguarding, storage, and destruction of sensitive customer information. [redacted]

Does Verizon limit the use and disclosure of customers' personal information?

Staff believes that Verizon's system which masks customer social security and driver's license numbers immediately upon entry into the system is exemplary. Use of the Verizon interactive telephone system to initiate automatic bill payment is also praiseworthy.

Verizon customer service has adequate and appropriate operational policies, practices, and procedures in place to specifically address the proper use, disclosure, and retention of sensitive customer data. [redacted]

Formatted: Font color: Auto

Managers also stated that they limit the risk for unauthorized use or disclosure of sensitive customer information by regularly monitoring internal controls and take appropriate corrective measures immediately upon discovery of any risk. Managers and supervisors review and regularly monitor software applications, programs, workstation conduct and employee access to sensitive information in an effort to minimize risk.

Managers must report any changes to employees' status or access authorizations immediately to IT. In the event of termination of an employee is required for any reason, revocation of access rights is coordinated between IT and the manager so that there is no window of opportunity for the terminated employee.

[redacted]

Company policy prohibits mention of sensitive customer information with anyone other than the account holder or persons authorized by the account holder. [redacted]

[redacted]

Do any employees have access to customers' personal information at off-site facilities?

Select managers, IT, and security employees have access to the network from off-site locations. [redacted]

Formatted: Font color: Auto

What controls has Verizon put in place for remote access of customer personal information?

Verizon stated that it has the proper controls in place to limit remote access to those with a valid business need-to-know, mitigate risk, and thwart unauthorized access. Remote access is only possible after receiving appropriate approvals by both management and IT Security. [redacted]

Remote access requires the use of [redacted]

[redacted]

Verizon does not currently have a work-from-home program for customer service. The company stated that there is no plan under consideration for such a program. No CSRs are authorized to access the customer service application from off-site.

5.2 Information Technology Controls

Has Verizon established an appropriate data security management function?

Verizon has established the Verizon Information Security Council (VISC) comprised of representatives from Verizon business units and company security support organizations. The group provides management direction and executive level steering for security programs.

Other organizations within the company hierarchy associated with information or network security include:

[redacted]

Verizon policies and procedures emphasize that information control security is the responsibility of every employee. Management asserted that all Verizon employees are responsible for safeguarding individual customer communications and information. Information Management (IM) has the responsibility to assess the risks and potential vulnerabilities to the overall network and individual workstations. IM managers assist operations managers in determining the feasibility of policies, practices, and procedures relative to the handling, retention, and protection of sensitive customer data.

[redacted]

Has Verizon established appropriate information security policies, procedures, and guidelines?

Adequate written policies for privacy and data security exist, although some date back as far as 2001. In the dynamic world of information security, this time gap between updates may be too excessive. As part of this review, Verizon provided:

- *CPI-810, Verizon Information Security*
- *CPI-810, Verizon Information Security Corporate Policy – Instruction*
- *CPI-810, Schedule D, Disposition of Personal Computing Assets*
- *CPI-810, Appendix A, Information Security Classification Schema*
- *CPI-810, Appendix B, Password Requirements and Responsibilities*

The following policies relevant to customer data security and protection of sensitive customer information were subsequently made available for staff review in the Verizon Tallahassee corporate offices:

- *CPS-130, Records Management*
- *CPS-301, Verizon Compliance Programs*
- *CPS-303, Verizon Privacy Principles*
- *CPI-303, Privacy Protection for Sensitive Information*

[redacted]

Verizon employs a layered 'defense in depth' to safeguard the network and the sensitive customer information it contains. Both [redacted] are in daily, continual use.

As part of this [redacted] IT manages:

[redacted]

Formatted: Highlight

[redacted]

Does Verizon limit physical access to customer information data resources through access authorization procedures, monitoring devices, and alarm systems?

For comprehensive security of sensitive customer information to exist, Verizon states that the company embraces the idea of synergy between physical and virtual security. [redacted] Training, policies, and procedures address access to facilities and physical security. There are written disciplinary standards for violations.

Staff visits to the Network Security facility, located in [redacted], and the Customer Sales and Service Center (CSSC) in [redacted] indicated that each facility has an adequate and appropriate level of physical security, based on function and sensitivity of the information handled. Both facilities require that visitors sign-in and be escorted by Verizon employees at all times. [redacted] Guests receive only temporary, adhesive identity badges. These are clearly distinct from those carried by employees; an unattended visitor would be quickly and clearly discerned.

Does Verizon restrict access to customer information related software functions, data, and programs?

The network and applications are protected by a full complement of security procedures necessary to gain access. Each authorized user is provided a unique identification credential and password. [redacted]

[redacted] Results are reviewed by IM technicians and available to management. According to Verizon policy and procedures, anomalies that suggest a possible security breach must be reported immediately and investigated fully.

Does Verizon monitor software security activity and produce appropriate management reports?

[redacted]

5.3 User Awareness and Training

Does Verizon have adequate privacy and data security policies and procedures?

Most written policies provided by Verizon offer little discussion of safeguards specific to sensitive customer information. Instead, the policies generally demonstrate an orientation toward the privacy and security of Verizon proprietary information.

Some written policies are old, and in the dynamic environment of modern technological change and cyber-security concerns, these may be of diminishing value or simply outdated. *CPI-810* series was published in 2001 and, so far as can be discerned, has never been updated. If this and other security-related policies and procedures have not undergone a thorough vetting since the early part of this decade, staff believes it would be wise to schedule such a review.

Most Verizon policies covering data security issues also do not provide a focused discussion about the protection of sensitive customer information. Instead, these policies demonstrate an orientation toward company privacy and the protection of Verizon proprietary information. Although the majority of privacy and data security policies currently in use do not specifically address the protection of sensitive customer information, Verizon management states that it believes existing materials help create an overall corporate attitude of awareness for safeguarding sensitive information. Staff believes Verizon should thoroughly review current policies and procedures, determining whether they are adequate for comprehensive protection of sensitive customer information.

Staff believes that Verizon's policy of reaffirming employee acknowledgement of the Code of Conduct and business ethics only upon "significant change" is also inadequate. Verizon employees could only estimate that such changes and the corresponding reaffirmation occurs approximately every three years. This is an inordinately extended period of time between affirmations of a critical component to the security of sensitive customer information.

Are Verizon employees properly trained on privacy and data security policies?

Newly hired Verizon employees receive a variety of mandatory training during their first month. Included in this training are elements on customer privacy and security of data of all types, including sensitive customer information. This web-based training is tracked and verified by a supervisor.

The web-based Verizon *NetLearn* system addresses privacy training, employee and manager requirements, general security awareness, and records management. Code of Conduct training is also mandatory via *NetLearn*.

CPI-303 Privacy Protection for Sensitive Information training is also mandatory for all new employees. Thereafter, a signed acknowledgment is required and training is updated on a recurring basis, but Verizon states this is done only when significant policy changes occur. Staff was informed that this occurs about every 2.5 to 3 years. It is not clear what constitutes significant policy change. Staff is concerned that this may also be an inordinately extended period of time between retraining and reaffirmation of a critical component for security of sensitive customer information

Management does provide periodic information security and privacy policies reminders through company e-mail, bulletin boards, and newsletters. These reminders can be universal, or targeted to business groups or functionalities.

Does Verizon have policies and procedures in place which address penalties for violations of privacy or data security policies?

CPI-810 Verizon Information Security, Chapter 6.3.5 states that Verizon Human Resources and Verizon Legal must ensure there exists a formal disciplinary process for violation

of organizational security policies, practices, and procedures. Violations can result in punishment up to and including dismissal as documented in the *Code of Business Conduct* and/or contracts. Additionally, violators could be subject to civil suit or criminal prosecution. These conditions apply not only to those who might violate the policies or procedures, but equally to those who condone misconduct, or who do not report it. The same conditions apply to supervisors and managers who fail to take reasonable measures to prevent, detect, or address misconduct related to sensitive information security information. Verizon also has policies in place to punish those who might seek to retaliate against those who in good faith reported potential misconduct.

5.4 Outsourcing Controls

Does Verizon provide third parties with access to customer personal and / or banking information?

Authorized third parties are granted access to internal Verizon systems on the same [redacted] basis which governs all other access. Verizon maintains that requests for third party access are carefully investigated prior to approval. Access is authorized on a case-by-case basis. Access credentials and scope are dependent on the job the third party vendor is hired to perform.

Controls, such as ID and passwords, are approved and authorized by Verizon management. In the event remote access is required by a third-party, access is allowed only using [redacted] software. [redacted]

Section 4.2 of *CPI-810 Verizon Information Security ("Security of Third Party Access")* applies and details relevant procedures. Verizon stated that a security risk assessment should be completed for all requests for third party access. This assessment is necessary to fully identify security requirements, controls, vulnerabilities, vendor security protocols, and the security implications of such access to the specific business unit and the overall network. Verizon's security policies and standards are clearly detailed in third party contracts. Contracts also note any required vendor employee security training.

External auditors for the company may be granted access to customer information on an audit-by-audit basis. Such access, as with all third parties, is predicated on a validated business need-to-know. Auditors are provided only that level of access required to perform the audit tasks assigned.

What controls has Verizon put in place to prevent disclosure of customer's personal information by third parties?

Confidentiality clauses are used when contracting for any third party service, support, or audit. Such clauses require third party employees to adhere to the same policies and procedures as Verizon employees when handling sensitive customer information. [redacted]

[redacted]. Third party employees are required to read and acknowledge the same privacy policies and ethics standards as employees of Verizon. Company management believes these measures reduce risk to acceptable levels and adequately safeguard sensitive customer information.

Verizon now requires Suppliers to be precluded by contract from accessing or storing information outside the United States without approval. They are required to comply with applicable U. S. or foreign laws, including laws governing the protection of sensitive personal information and financial information.

In addition, Verizon has adopted a Supplier's Code of Conduct which mandates that suppliers adhere to certain standards of conduct, including ethical standards, to safeguard confidential information. This requirement extends to customers' private, sensitive information. . The privacy protections in the Suppliers' Code of Conduct are comparable to the Code of Conduct governing Verizon employees.

5.5 Auditing Controls

Does Verizon possess, or have access to, competent auditing resources to evaluate information security and associated risks?

Verizon employs a full-time staff of internal auditors. Verizon asserted that it seeks qualified individuals with appropriate certifications for its audit staff. Each member of the audit staff is provided a minimum of [redacted] hours annually for continuing education. [redacted] Verizon indicated that its audit organization has approximately [redacted] employees. The organization is led by the Senior Vice President – Internal Audit [redacted] The Senior Vice President reports to the Audit Committee of the Board of Directors and reports administratively to the Chief Financial Officer.

Formatted: Font color: Auto

An audit plan is prepared annually and presented to the Verizon Audit Committee. This committee has approval authority for the overall plan.

Does Verizon periodically assess the organization's information security practices?

Verizon management, in coordination with the IM group, regularly assesses information security practices [redacted] systems help simplify and automate this process. [redacted]

Verizon internal auditing also conducts periodic, formal assessments and audits to identify vulnerabilities and existing safeguards.

The company adheres to the [redacted] program. One requirement is to regularly monitor and test networks. This

applies to any network, component, server, or application that contains cardholder information or sensitive authentication data.

Verizon is also a licensee of [redacted] is an independent, nonprofit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information. This watchdog organization has the reputation for promoting privacy policy disclosure, informed user consent, and consumer education. [redacted]

During 2006 and 2007, Verizon conducted [redacted] audits which dealt with aspects of sensitive customer information. The company furnished a synopsis of each audit, the noted deficiencies and management response. All deficiencies noted during the audits have been remediated. Audits conducted in 2006 and 2007 included:

[redacted]

Has management provided assurance that information security breaches and conditions that might represent a threat to the organization will be promptly made known to appropriate Verizon corporate and IT management?

Verizon states that any breach or attempted breach must be reported immediately to a central reporting and response organization called CIRT (Computer Incident Response Team). CIRT is responsible for incident awareness, reporting, and has the lead for incident remediation. The CIRT has authority to gather the necessary experts to thoroughly investigate the problem and manages the remediation until the incident is closed. Sections within *CPI-810 Verizon Information Security* and *CPI-810, Verizon Information Security Corporate Policy – Instruction* provide complete incident reporting criteria.

Verizon Investigations uses a case management system called [redacted] to track incidents of potential sensitive information compromise. The company listed the following incidents in Florida during the period reviewed:

Each case was investigated by Verizon Security. In each case, a stolen/missing equipment checklist was provided to Verizon Cyber Security for review. Cyber Security passes this information to the Verizon Privacy Office. Investigators in the Privacy Office review the checklist for any indication of exposure or breach to sensitive information.

In the event of hardware or data loss, Verizon Security reviews the case and makes corrective action recommendations to management. These recommendations are aimed at preventing similar, future losses and to mitigate potential data compromise. For thefts, Security refers the incident to law enforcement and assists in the investigation, as required.

According to the company, none of the incidents during 2006 and 2007 endangered the Verizon network, its applications, or sensitive customer information.

5.6 Conclusions

Verizon has policies, practices, and procedures in place to protect sensitive customer information. Company management acknowledges its own overriding responsibility for information security while using multiple methods and media to instill a similar sense of individual responsibility in every employee. Virtual and physical security now in use are in keeping with the best industry practices, layered for a defense in depth, and appear to be effective.

Staff believes that Verizon's masking of social security numbers in all customer service applications is exemplary. So, too, is the interactive voice system which allows customers to set up credit or debit bill payment. This eliminates the need for customer service representatives to process any banking information and eliminates all risk of compromise to such data.

However, staff does have some concern about two items connected with Verizon policies relevant to sensitive customer information. These concerns center around two issues:

- Written security policies do not contain appropriate emphasis on *customer* sensitive information security and some have not been updated for five years or more
- Employee Code of Conduct and business ethics affirmations are not regularly updated on a set schedule

"Staff believes that Verizon's masking of social security numbers in all customer service applications is exemplary."

Most Verizon policies covering data security issues also do not provide a focused discussion about the protection of sensitive customer information. Instead, these policies demonstrate an orientation toward company privacy and the protection of Verizon proprietary information. Although the majority of privacy and data security policies currently in use do not specifically address the protection of sensitive customer information, Verizon management states that it believes existing materials help create an overall corporate attitude of awareness for safeguarding sensitive information. Staff believes Verizon should thoroughly review current policies and procedures, determining whether they are specific and adequate for comprehensive protection of sensitive customer information.

Some written policies are old, and in the dynamic environment of modern technological change and cyber-security concerns, these may be of diminishing value or simply outdated. *CPI-810* series was published in 2001 and, so far as can be discerned, has never been updated. If this and other security-related policies and procedures have not undergone a thorough vetting since the early part of this decade, staff believes it would be wise to schedule such a review.

Staff believes that Verizon's policy of reaffirming employee acknowledgement of the Code of Conduct and business ethics only upon "significant change" is also inadequate. Verizon employees could only estimate that such changes and the corresponding reaffirmation occurs approximately every three years. Staff believes this an inordinately extended period of time between affirmations of a critical component to the security of sensitive customer information. Staff recommends that such reaffirmations occur at least biannually.

CPI-810 Appendix B -Verizon Password Requirements and Responsibilities	November 2001	Currently being updated.
CPI-810 Schedule - Disposition of Personal Computing Assets Policy	November 2001	Revised version released January 2008.
Your Code of Conduct	Updated in 2002 and 2006	Update planned for 2009.

As this table shows, Verizon's security policies have been recently issued, are in the process of being updated or have updates planned in the near future. Verizon thus is keeping its security policies up to date.

Policy Focus on Sensitive Customer Information

Verizon's policies address customer sensitive information comprehensively. The policies address how to classify, protect and appropriately handle every piece of information that Verizon deals with, including customer sensitive information, from the time it is received to the time it is destroyed. The 810 series of policies addresses the fundamentals of network and data security, the classification of information for handling purposes, password protections and the proper disposal of computing assets. Series 810 has also been supplemented with new polices including CPS-303 and CPI-303, both of which focus on the protection of customer sensitive information.

CPS-810, entitled "Information Security," established guidelines for Verizon and its subsidiaries for the protection of Verizon's information assets and data and the systems used to create, store, and communicate data, including Verizon customer data and data provided to Verizon by business providers.

CPS-303, entitled "Verizon Privacy Principles," sets forth the commitment of Verizon and its subsidiaries to safeguard customer information and to provide customers with an understanding of how their confidential information will be used by Verizon. Ten Verizon Privacy Principles express Verizon's commitment to strong and meaningful customer privacy protection in an era of rapidly changing communications technology. These Principles are guidelines to help us work with our customers to make appropriate use of customer information acquired through a variety of means. The goals of this policy are to comply with all applicable laws and regulations and to balance our customers' concerns about privacy with their interest in receiving quality service and useful new products.

CPI-303, entitled "Privacy Protections for Sensitive Personal Information," describes the required practices necessary to strengthen Verizon's privacy compliance mechanisms for protecting certain personally identifiable Sensitive Personal Information. CPI-303 provides *minimum* requirements for protection of Sensitive Personal Information, defined as any one or more of the following four data elements that when combined with data that can be used, either alone or through other readily available data, to identify an individual:

1. social security number (SSN)
2. financial account number (i.e. credit card number or bank account number)
3. driver's license or state issued identification number

4. health care records

In short, Verizon's data security policies deal with customer sensitive information in a systematic, comprehensive and effective way.

Frequency of Employee Affirmation of the Code of Conduct

Verizon has a comprehensive Code of Conduct that upholds Verizon's commitment and core values to put customers first, act with integrity, treat people with respect, be accountable and set a high bar for performance excellence. The Code of Conduct addresses the handling and protection of customer information along with many other important ethical principles. All employees are required to complete Code of Conduct training and acknowledge their understanding of and agreement to adhere to its standards. The Code of Conduct is required to be reviewed immediately by new employees followed by the mandatory Code training once they begin working for the company and affirmed when updates are made. The latest updates to the Code of Conduct occurred in 2002 and 2006 and tentative plans are to review and reissue the code with retraining in 2009. In addition to being certified regarding the Code of Conduct, employees are required to take the following mandatory training courses applicable to their job classification that reinforce the protection of customer sensitive information between updates:

- Management Code of Conduct Training – Course code YYJ91098NL – 2006: Covers the responsibility for protecting data, records and all communications entrusted to an employee's care by Verizon, its customers or its business partners (Parallel course for Associates is YYJ91099NL).

- Security Awareness Top Ten – Course code YYJ90963NL – 2006: Identifies the employee's role in securing Verizon networks and systems (including customer information); also references CPI-810 (All employees).

- Corporate Compliance – Privacy – Course code YYJ91208NL – 2007: Summarizes the context and scope of Verizon's Privacy obligations and details the requirements of a new Verizon policy instruction on Privacy-Corporate Policy Instruction CPI - 303 (Management employees).

- Corporate Compliance – Records management – Course code YYJ94000NL – 2008: Summarizes Verizon's policies, the laws and the records retention schedules that govern the protection of proprietary and customer information. The proper disposition of paper, electronic records and computing assets also is addressed (Management employees).

The Code of Conduct is frequently reviewed by Verizon's Ethics Office and Legal Department and updates are made when required. Important principles are reinforced with employees through supplemental mandatory courses like the ones mentioned above. We also use the corporate eweb as well as e-mail messages and newsletters to remind employees about the Code of Conduct and communicate a series of Code related articles and reminders to employees on this topic. For example, the e-communication below issued in early2008 was a reminder to all employees to review and be familiar with the Code of Conduct. The e-mail stated:

Supervisors: Please share this communication with employees who do not have email access.

For Verizon to continue to win in the marketplace, each employee must conduct business in a manner that strengthens our culture of integrity and the Verizon brand. The *Verizon Code of Conduct* is your guide for understanding Verizon's standards of business conduct. All employees are expected to adhere to the standards of the Code and our Core Values of Integrity, Respect, Accountability and Performance Excellence.
Please make sure you are familiar with the Code. Review your copy again or you can access the Code of Conduct on About You. If you have any questions or concerns, please contact your supervisor or call the VZ Ethics and EEO GuideLine at 800-856-1885 or on-line at https://www.verizonguideline.com/.

Failure to comply with any provision of the Code of Conduct or company policy is a serious violation, and may result in disciplinary action, up to and including termination, as well as civil or criminal charges. These consequences may apply not only to employees who violate the Code, but also to those who condone misconduct, fail to report or take reasonable measures to prevent, detect and address misconduct, or seek to retaliate against those who in good faith report potential misconduct.

In short, requiring the initial affirmation that an employee will comply with the Code of Conduct, followed by reaffirmations when substantial changes are made, is sufficient to ensure that employees understand and agree to comply with it. The ongoing training and messaging that Verizon provides relating to the Code of Conduct reinforces the requirement of continued compliance and ensures that employees remain mindful of that responsibility.

APPENDIX A

This chart summarizes each company's security policies, practices, and initiatives. The points are discussed in more detail in each respective company chapter.

Florida ILEC Customer Sensitive Information Security Practices			
	AT&T	Embarq	Verizon
Access lines in Florida			1.3 million
Emphasis on data security (new employee training, ethics standards instruction / statements, coaching, and supervision)			Yes
Proactive data security programs (IT and Customer Service)			Yes
Audit of IT / Customer Data operations in the last 24 months			Yes
Number of security breaches, last 24 months			0
Number of IT auditors			[redacted]
Employs IT "defense in depth" using a combination of Intrusion Detection, Intrusion Prevention, virtual and physical measures to counter risks			[redacted]
Masking of customer social security numbers (SSN)			Yes, all digits
Total number of employees			[redacted]
Number of employees with access to customers' social security numbers			[redacted]
Work-at-home program for Customer Service Representatives			No
Share customer account information with an authorized third party over the telephone			[redacted]

Source: Company Responses to Staff Document Request

APPENDIX B

Appendix B summarizes the sensitive customer information collected and used by the three Florida ILECs subject to this review. More detailed discussion is in respective company chapters.

Florida ILEC Sensitive Customer Data				
	Collects	Uses	Masked	Notes
AT&T				
Social security number (SSN)				
Driver's license number				
Bank or Credit Card Info for Auto-pay				
Date-of-Birth				
Embarq				
	Collects	Uses	Masked	Notes
Social security number (SSN)				
Driver's license number				
Bank or Credit Card Info for Auto-pay				
Date-of-Birth				
Verizon				
	Collects	Uses	Masked	Notes
Social security number (SSN)	[redacted]	[redacted]	[redacted]	
Driver's license number	[redacted]	[redacted]		[redacted]
Bank or Credit Card Info for Auto-pay				[redacted]
Date-of-Birth	[redacted]	[redacted]	[redacted]	[redacted]

Notes:

1. [redacted]

STATE OF FLORIDA

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

CONFIDENTIAL

Public Service Commission

ACKNOWLEDGEMENT

DATE: June 13, 2008

TO: **Dulaney L. O'roark, Iii, Verizon**

FROM: **Ruth Nettles, 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** Costomer Data Security of Florida Incumbent Local Exchange Carriers Draft Report, **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.