REDACTED

MAY 2008

080000-OT

SURVEY OF

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

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.

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

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.

[redacted]

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.

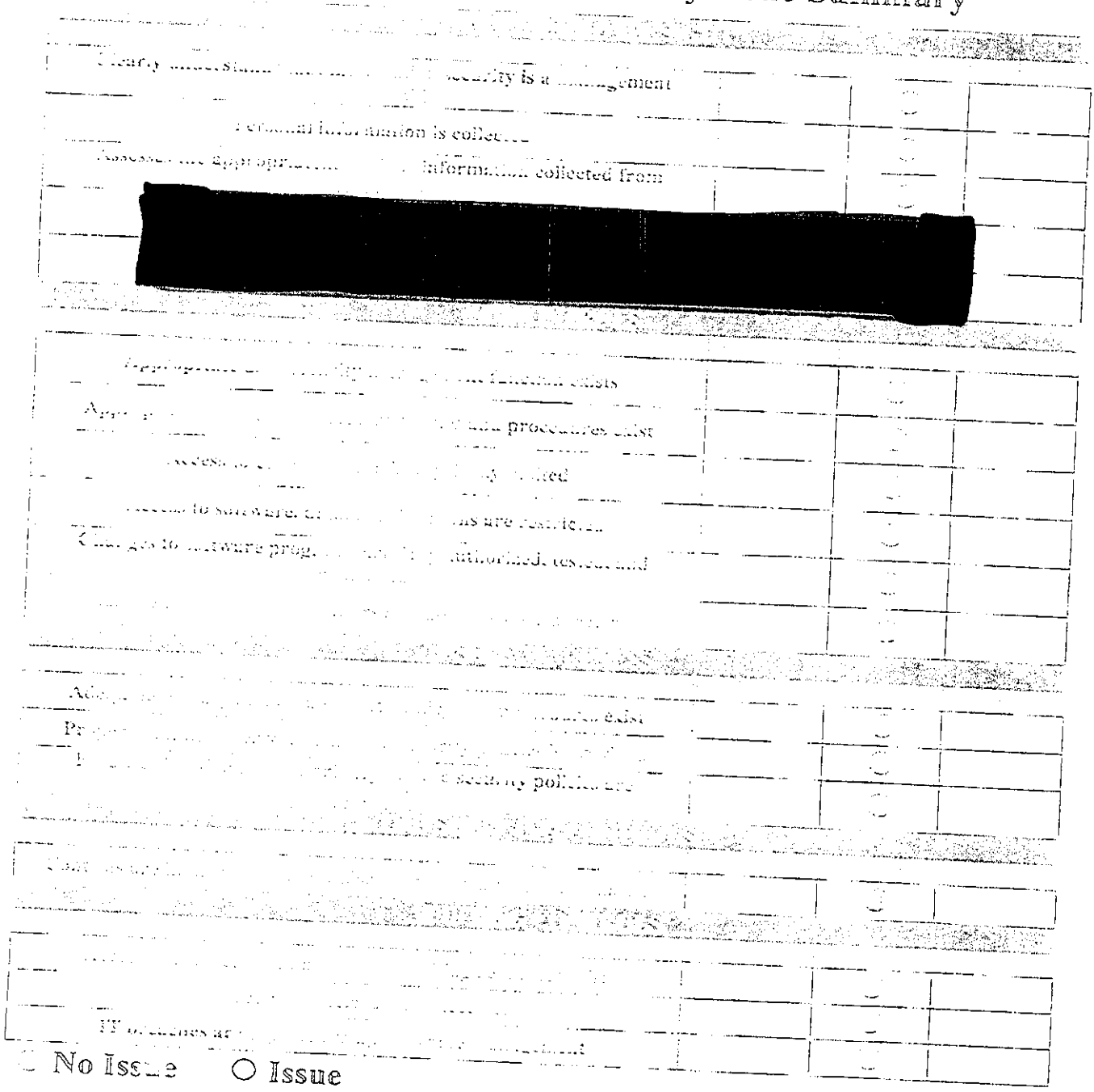
"None of the reviewed companies reported, or are aware of, any major breaches involving sensitive customer information in the previous two years. . . ."

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



○ No Issue ○ Issue

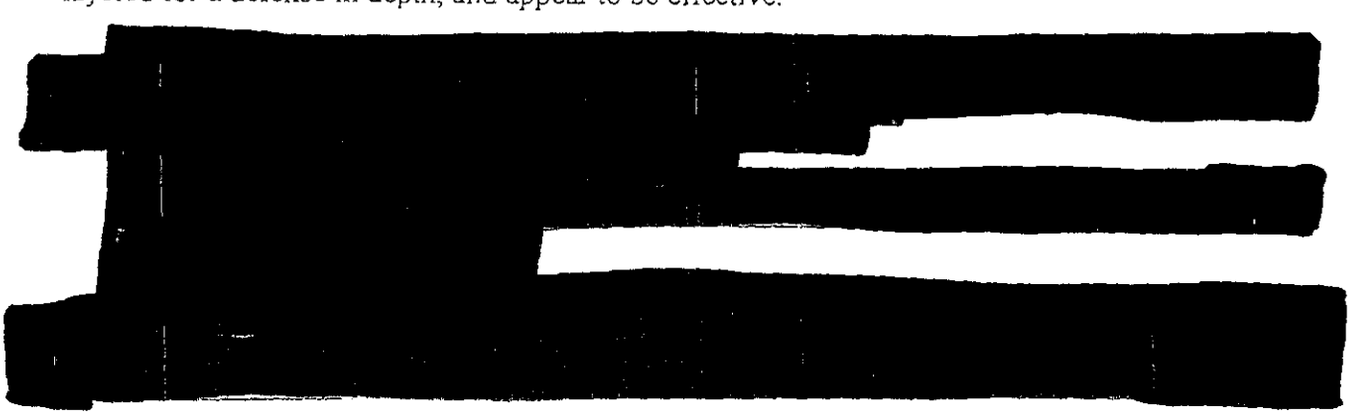
[redacted]

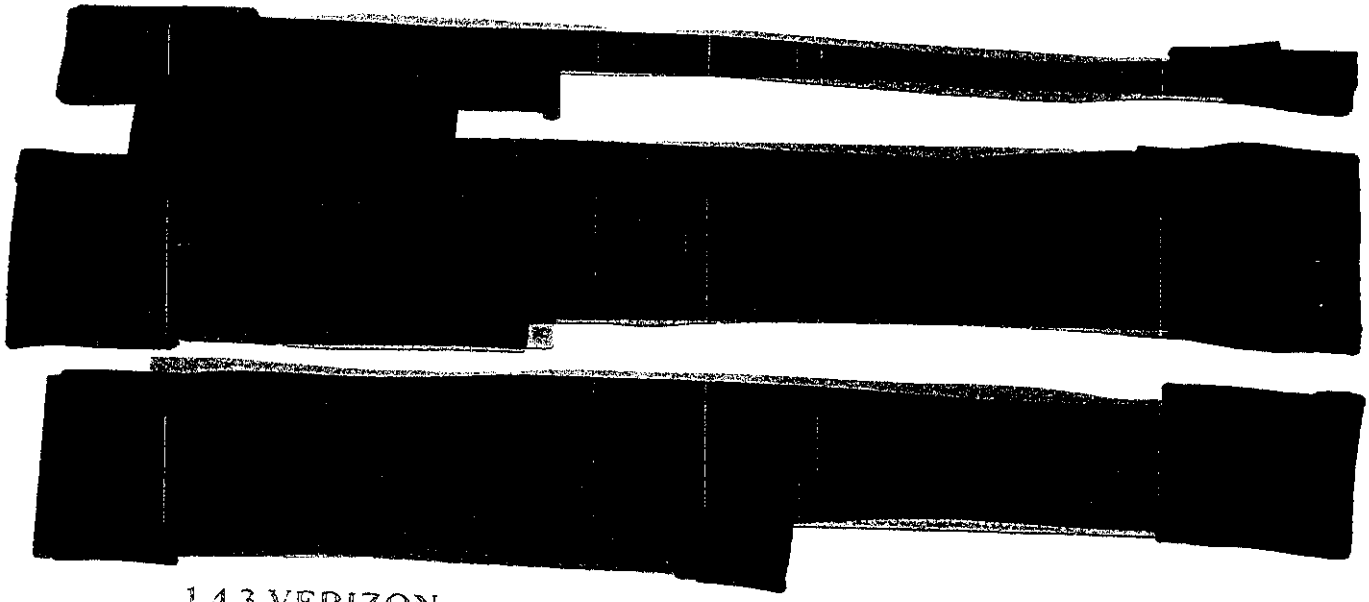
1.4.1 AT&T

1.4.2 EMBARQ

Embarq has developed and implemented policies and procedures that focus on protecting confidential information. The company also has adequate measures in place to secure its physical assets by monitoring and restricting access to specialized areas by job type and need-to-know. Embarq also proactively protects its network and the sensitive information stored therein using both external sources, and its own internal security

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.





1.4.3 VERIZON

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 Survey

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.[3]

[3] *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.[4]

"...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:

2002	[illegible]
2003	14,119
[illegible]	[illegible]
2005	17,048
[illegible]	[illegible]
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.[5]

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.[6]

[illegible]

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

[4] Identity Theft Victim Complaint Data, Florida, January 1 – December 31, 2006, FTC, Washington, DC, Fig 4a
[5] *2006 FTC Identity Theft Survey Report, November 2007*
[6] 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."[7]

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.

[7] *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.

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.[8] 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."[9] 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."[10] The Task Force has recommended the development of a comprehensive record on private sector use

[8] Public Law 105-318,112 Stat.3007 (October 30,1998)
[9] The President's Identity Theft Task Force, Combating Identity Theft – A Strategic Plan, 2007, p. viii
[10] 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. [11]

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 IOU 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.

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

4.0 Embarq

Embarq Corporation is headquartered in Overland Park, Kansas, and has approximately 19,000 employees operating in 18 states. In Florida, Embarq currently services approximately 1.3 million residential customers. Embarq's service portfolio includes local voice and data services, long distance, Business Class high-speed Internet, wireless, enhanced data network services, voice and data communication equipment, and managed network services.

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

Embarq's responses to document requests and on-site interviews indicate that management does have a clear understanding that information security is primarily a management responsibility. Embarq has employed a system that identifies an Information Asset Owner (IAO) who is personally responsible for the security, distribution, and access to specific sensitive customer information. IAO's throughout Embarq are typically at the level of Director. This places Embarq's management within the information chain of custody, charging them with the day-to-day responsibility of sensitive customer data security.

Embarq's commitment to protecting sensitive customer data is highlighted in the privacy principles it employs to assure their customers that the information collected is used only for appropriate purposes, and is protected from any inappropriate use or disclosure.

What type of personal information does Embarq collect from customers?

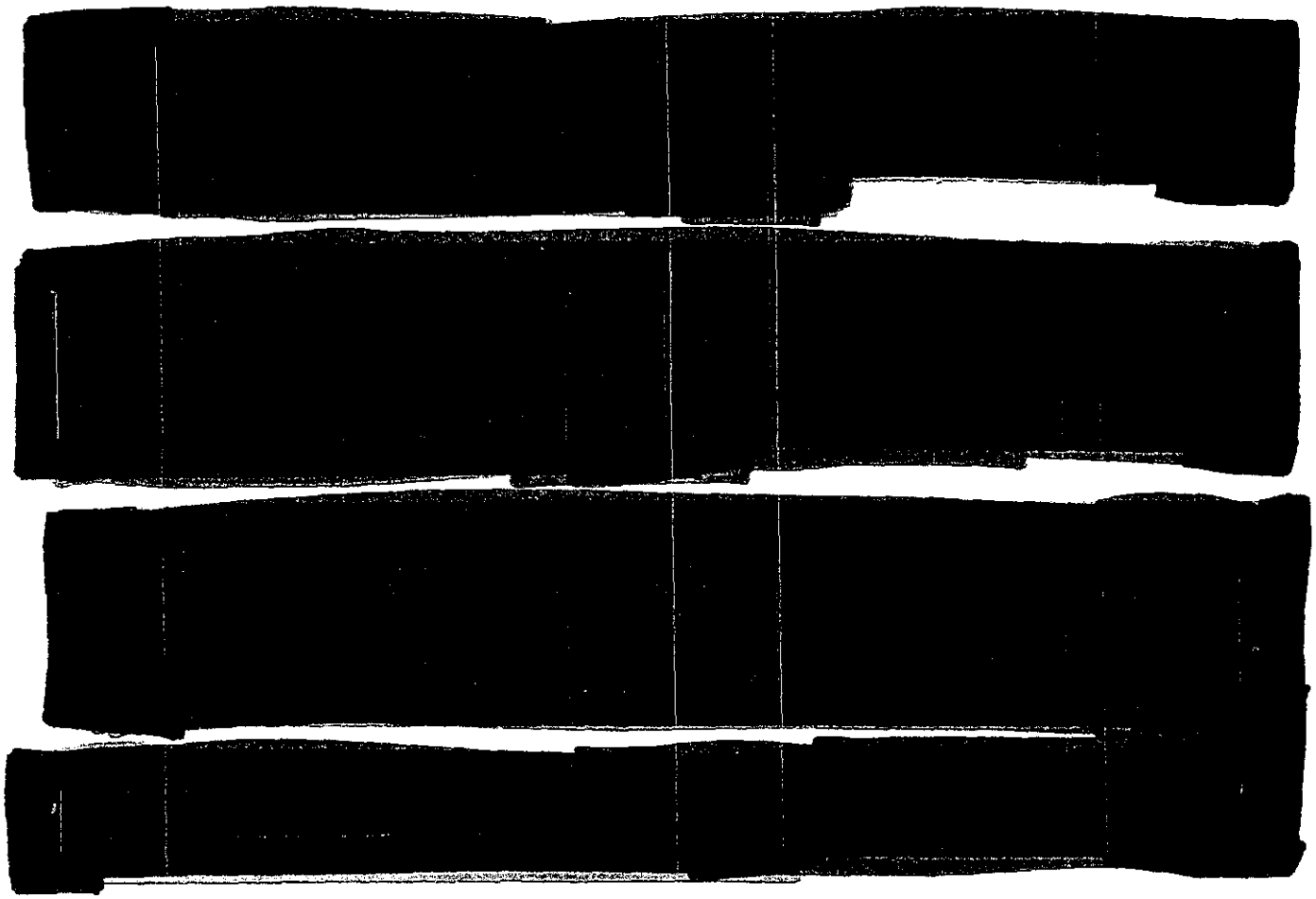
When initiating a new residential account, a Customer Service Representative (CSR) collects the customer's information [redacted]

The customer may also be asked to provide a previous address. The same information is collected on any co-applicant who will be sharing responsibility for bill payment. The customer can elect to provide a credit card number or account number to pay for any account set-up fees and/or establish automatic billing.

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

Embarq's responses to staff's data requests and interviews indicated that management has assessed the information collected and deemed it to be appropriate to processing new account requests, and essential for processing service requests and providing telecommunication services. Embarq's management states it is aware of the potential risks associated with collecting such information, especially with individual social security numbers that are specifically collected in order to run a customer credit worthiness check. The number is then maintained in the system for customer identification purposes.

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



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

[redacted]

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

[redacted]

Has Embarq established an appropriate data security management function?

According to Embarq, all information is assigned directly to an Information Asset Owner (IAO), who is normally at the level of Director within Embarq. The IAO is responsible for protecting any information assigned. Each IAO can delegate authority for day-to-day operational use, but delegation of the responsibility for information security is prohibited. The

overall responsibility remains with the IAO until the information is verified to be properly destroyed, or it is assigned to another IAO. This system provides a constant and traceable chain of custody leading to those charged with the protection of Embarq's internal data, proprietary information, and sensitive customer information.

Embarq management believes that the protection of sensitive customer data is vital to its business success. The company uses a number of monitoring tools to evaluate the overall integrity of the information system. These tools include an in-line intrusion prevention system to identify, deter, or prevent unauthorized entry. All access to the system is monitored by Security Event Monitoring and any unusual event detected is investigated by the Computer Incident Response Team (CIRT).

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

Embarq has established appropriate information security policies, procedures, and guidelines by employing logical access controls based on job responsibilities and work-related "need-to-know." Storage and handling procedures are detailed in Embarq's *Information Classification Guidelines and Information Classification & Quick Reference Guide*, published March 2007.

The *Enterprise Security Policy* addresses topics such as:

- Information Classification
- Cryptographic Controls
- Network Security
- Access Control

The *Information Security Standards* outlines:

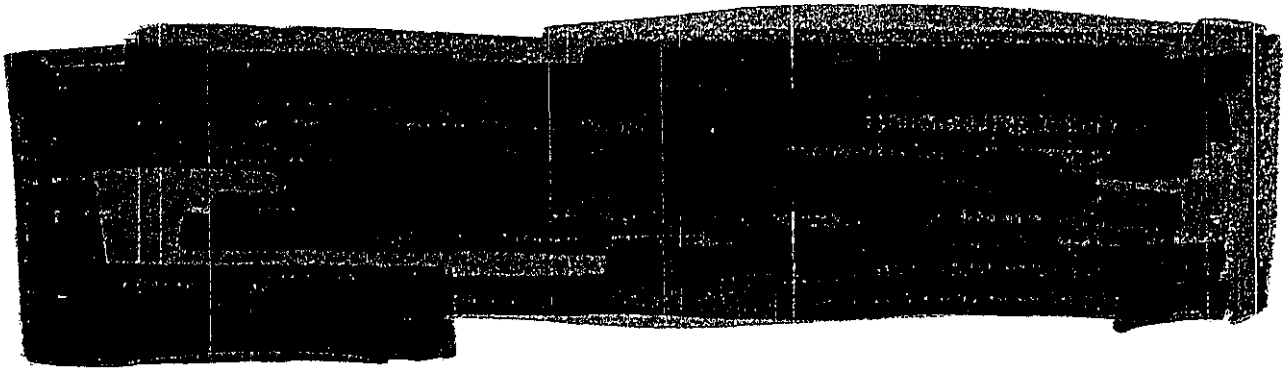
- Data Classification, Handling, and Storage
- Encryption of Electronic Information
- Information Communications
- Network and Computing Systems
- Risk Management
- Security Compliance Reviews
- Third Party Services.

Information Technology employees work to protect sensitive customer information and to make the entire network resistant to penetration by running the most current versions of software available. Software upgrades, commonly called "patches," are received regularly [redacted] These updates are received daily and reviewed by Embarq Information Technology. For any level of Critical Alert or Alert, the CIRT team becomes involved to take measures to handle the security threat. Embarq also receives notices directly from Microsoft due to the significant number of Windows-specific vulnerabilities.

According to Embarq, all identified critical vulnerabilities are tested and patches implemented [redacted] Other patches are applied during [redacted] Embarq also engages in regular [redacted] to test its own [redacted] These steps are proactive in nature to ensure the system is maintained ahead of technological advances employed to try to breach the system.

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

[redacted] Embarq's physical security strategy is based on a corporate-wide initiative that restricts the access of sensitive data to those with prior authorization and a need-to-know. While the security components can be site specific, they are generally in use throughout the company.



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

Embarq's network security is a multi-tiered system that requires the operator to be an authorized user with a pre-established need-to-know based on the approval of both management and information technology. Access to different functions of the network is derived from a menu at sign-on from each workstation, tailored to the individual users. Lack of the appropriate level of access authority will result in a failed sign-in attempt. Failed attempts are monitored and management is notified of attempted unauthorized systems access.

Embarq's *Enterprise Security Policy* defines the scope and controls by which ongoing assessments and continuous compliance monitoring are performed. The Security Compliance Team performs monthly vulnerability assessments on all critical systems and works with the appropriate agents to remediate any identified issues. Embarq also deploys 'defense in depth' security architecture, utilizing data protection resources such as network-based firewalls, an in-line Intrusion Prevention System, and a Security Event Monitoring system. Events that may pose a risk to the Embarq network may be blocked by the Intrusion Prevention System or sent to the

Security Event Monitoring system. The Computer Incident Response Team also proactively monitors the system for security events.

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

Embarq information technology has the ability to monitor employee access to the network and sensitive information in real time. This oversight provides IT the capability of determining who is accessing specific areas of the network, when such access occurred, the duration of the access and whether unauthorized users attempted access.

All access to Embarq's network system is retained in audit logs that are sent to Security Event Monitoring and are available for review. Unusual activity triggers an alarm for the Computer Incident Response Team to investigate and review. System access reports are generated quarterly for review by the Information Asset Owner (IAO), who verifies the information is accurate. While the reports are generated quarterly, unusual or suspicious activity is handled immediately and the IAO and appropriate management are notified prior to the scheduled quarterly report.

4.3 User Awareness and Training

Does Embarq have adequate privacy and data policies and procedures?

Annually, Embarq employees are required to read and acknowledge the *Code of Conduct* dated February 2007. Verification of the acknowledgement is handled electronically as employees must enter their user ID and password for the electronic signature. Employees also receive an annual refresher on handling sensitive customer data. However, the Embarq *Code of Conduct* only briefly addresses the handling of sensitive customer information and does not cite specific laws or regulations. Employees are referred to the *Employee Guide*, the *Privacy Policy* and the *Customer Proprietary Network Information Policy* for more details. Staff notes that Embarq does not have separate, written policies for sensitive customer information. However, staff does not believe this to rise to the level of a finding or major concern.

All employees must acknowledge the Proprietary Information Display on a daily basis as part of the initial sign-on process. While this is an affirmation of their responsibilities in handling CPNI, neither the Proprietary Information Display, nor the Code of Conduct specifically address the use of sensitive customer information. These policies include corporate information as a whole and include the protection of sensitive customer information only by mention of how the information should be used, rather than how it is to be protected.

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

New employees to Embarq are trained "from the ground up," reviewing and acknowledging all of the above listed policies and guidelines, as well as formalized training on

how to handle corporate information and sensitive customer information. The training is self-paced, using both classroom and intranet formats. Once areas of training have been completed, the employee's file is updated to note the completion.

Regular on-the-job training is used to reinforce those principles utilizing the corporate intranet, annual review, and acknowledgement of the *Code of Conduct* and CPNI training, and interoffice memos with topics highlighting any current areas of interest, including safeguarding sensitive customer data. Embarq states that it strives to bring the safeguarding of sensitive customer data and other proprietary information to the forefront of each employee's thinking.

[redacted]

Does Embarq have policies and procedures in place which address penalties for violations of Privacy or Data Security policies?

Embarq corporate policy, in the *Employee Guide, Policies and Procedures* states:

"Any employee who violates Company policy regarding the confidentiality of customer information will be subject to disciplinary action. Disciplinary action may include termination, even for the first offense."

Embarq's policy calls for any action that results in a breach of sensitive customer information to be referred to Human Resources for review and determination of the next course of action. For a breach involving electronic data, the Computer Incident Response Team is to become involved to investigate and communicate its findings for any further course of action.

[redacted]

Does Embarq provide third parties with access to customer personal or banking data?

Embarq partners with independent vendors located regionally throughout the country to assist in its customer service and billing needs. Customers in Florida who choose to mail in their bill payments send their remittance to Embarq's contracted payment vendor,

[redacted]

Customers also have several other options for making

payments. Customers can visit one of Embarq's 18 stores, log-on to Embarq's Web site or contact a call center to make a payment.

Embarq also contracts with several other vendors to allow multiple options for customer bill payment [redacted] Customers may inquire online about the service and then go to a participating retailer, such as Wal-Mart or Radio Shack, to purchase the prepayment. Embarq also allows payment through all Western Union locations.

Embarq enters into a *Master Agreement* with these companies that contractually binds the vendor to terms and conditions regarding the handling of any information provided to contractors. Embarq also maintains *Physical Security Administration: Standards for Suppliers*, dated October 2007, along with a *Supplier Code of Conduct*, also revised in October 2007. These documents further highlight Embarq's requirements for the vendor's responsibility for handling customer information, such as protecting confidential and proprietary information that belongs to Embarq and its customers, along with computer and network security.

What controls has Embarq put in place to prevent disclosure of customers' personal information by third parties?

Embarq states that each vendor operates under the same terms as defined by the *Master Agreement*. Each vendor is expected to secure customer information in a manner that is at a minimum, equivalent to Embarq's corporate standards, which are also supplemented by the *Physical Security Administration: Standards for Suppliers* and the *Supplier Code of Conduct*.

[redacted]

All third party employees that provide service to Embarq are required to undergo a background check. All third party vendor personnel are to abide by all policies and procedures applicable to Embarq premises access rights. Embarq states that its general practice is to ensure that everyone knows and understands its policies regarding security of confidential information and the *Code of Ethics*. Embarq releases these documents periodically and encourages review by both Embarq employees and all third party vendor employees.

Embarq's *Master Agreement* states all third party vendors must adhere to stringent, company-wide security standards and their internal structures are open to assessment by Embarq's security team. Violations or breaches of its confidentiality policies will result in corrective actions that include dismissal of contract agreements.

4.5 Auditing Controls

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

[redacted] Embarq's *Enterprise Security Policy* defines the scope and controls by which ongoing assessments and continuous compliance monitoring is preformed. The IT Security Compliance Team performs monthly vulnerability assessments on all critical systems and works with the appropriate agents to remediate any identified issues. All internal audit reports contain action plans that were agreed to by management and serve the same purpose as traditional management responses. Each action plan is associated with a specific Information Asset Owner and timeframe for remediation.

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

[redacted]

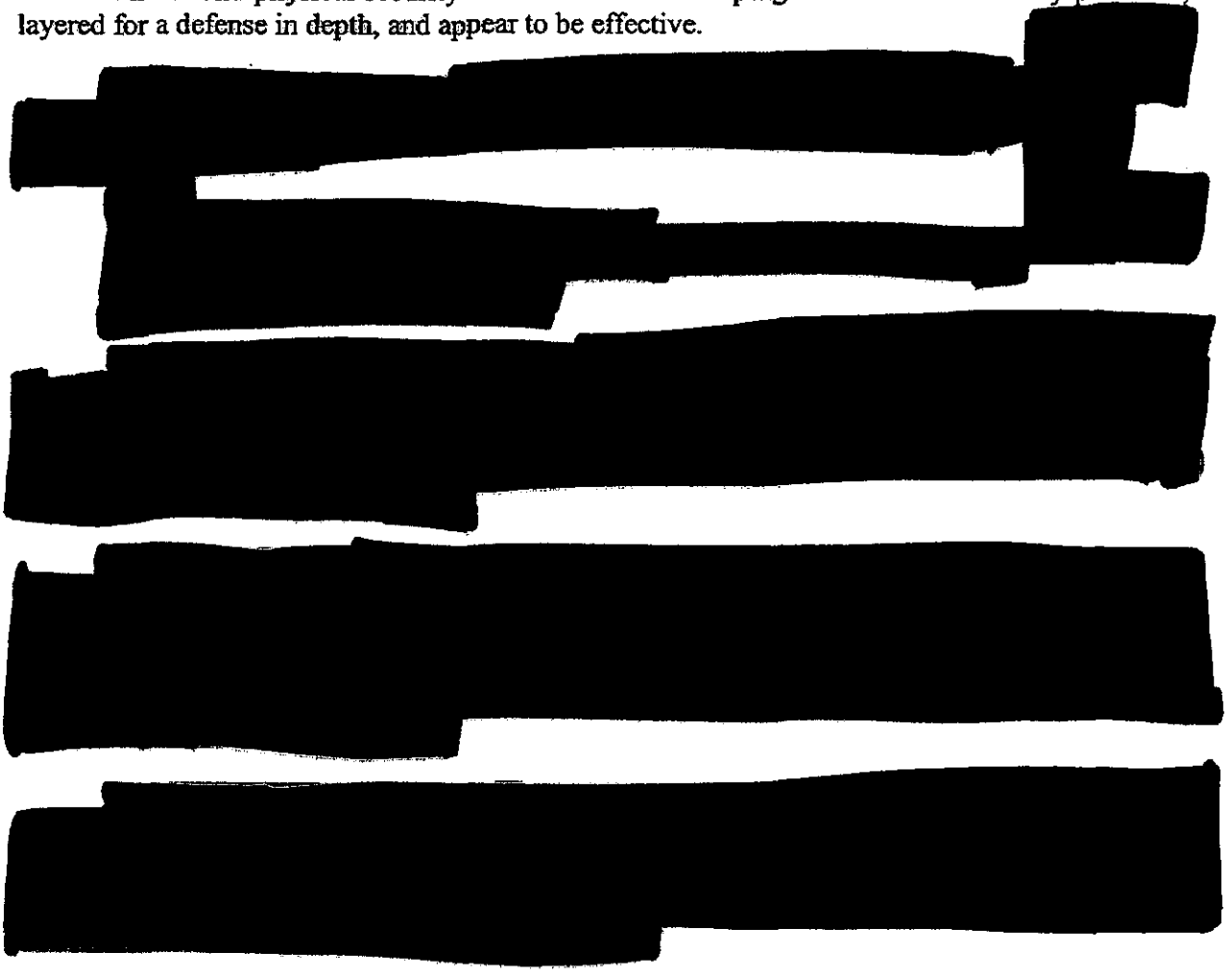
Has management provided assurance that information security breaches and conditions that might represent a threat to the organization will be promptly made known to appropriate Embarq corporate and IT management?

Embarq complies with Florida Statutes, Section 817.5681, which requires the company to notify customers in the event of a breach of customer personal information. Any potential breach of information is referred to Human Resources where the incident is investigated with the Computer Incident Response Team. A confirmed breach will also involve Embarq's legal team that will review the incident and begin any steps required to begin customer notification. Embarq's current system utilizing an Information Asset Owner provides a direct line of communication and notification through the corporate chain of command.

4.6 Conclusions

Embarq has developed and implemented policies and procedures that focus on protecting confidential information. The company also has adequate measures in place to secure its physical assets by monitoring and restricting access to specialized areas by job type and need-to-know. Embarq also proactively protects its network and the sensitive information stored therein using both external sources, and its own internal security

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.



6.0 Company Comments

This section provides a venue for companies to comment on the report. All comments have been reproduced verbatim.

[redacted]

To be determined.

[redacted]

To be determined.

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 [redacted] Customer Sensitive Information Security Practices

Access lines in Florida		1.3 million	
Emphasis on [redacted] employee [redacted]		Yes	
Proactive data security programs (IT and Customer Service)		Yes	
Audit of IT [redacted]		Yes	
Number of security breaches, last 24 months		0	
[redacted]		[redacted]	
Employs IT "defense in depth" using a combination of Intrusion Detection, Intrusion Prevention, virtual and physical measures to counter [redacted]		Yes	
[redacted]		[redacted]	
Total [redacted] employees		19,000 in eighteen states	
[redacted]		[redacted]	
Work-at-home program for Customer Service Representatives		Yes	
Share customer information with [redacted]		Yes, upon verification	

Source: Company Responses to Staff Document Request

APPENDIX B

[redacted]

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 [redacted]				
Date-of-Birth				
Embarq				
[redacted]				
Verizon				
Social security number (SSN)				
Driver's license number				
Bank or Credit Card info for [redacted]				
Date-of-Birth				

Notes:

[redacted]