MAY 2008

REDACTED

unredacted

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

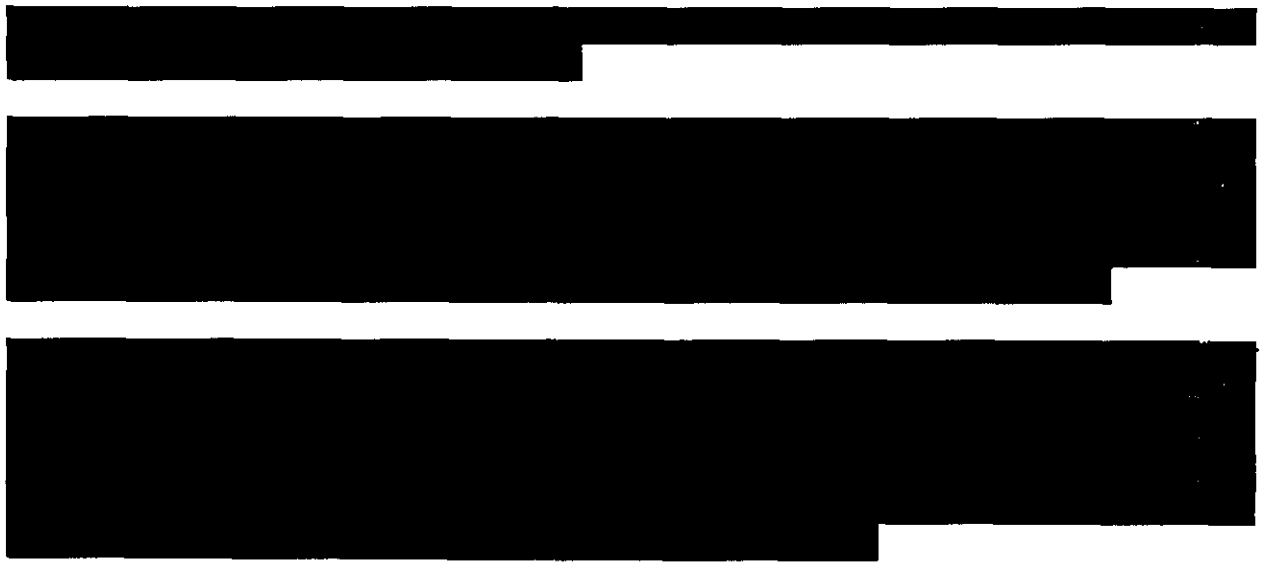
Table of Contents

Sensitive Customer Data Safeguards Controls

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

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[1] Excessive intervals between Code of Conduct affirmations, out of date security policies and a lack of focused policy discussion for customer-specific sensitive data security.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



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?

[redacted]

What type of personal information does Verizon collect from customers?

[redacted]

[redacted]

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

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

[redacted]

[redacted]

5.2 Information Technology Controls

Has Verizon established an appropriate data security management function?

[redacted]

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

[redacted]

[redacted]

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

[redacted]

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

[redacted]

[redacted]

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?

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

5.4 Outsourcing Controls

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

[redacted]

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

[redacted]

[redacted]

5.5 Auditing Controls

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

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

[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?

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.6 Conclusions

[redacted]

[redacted]

6.0 Company Comments

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

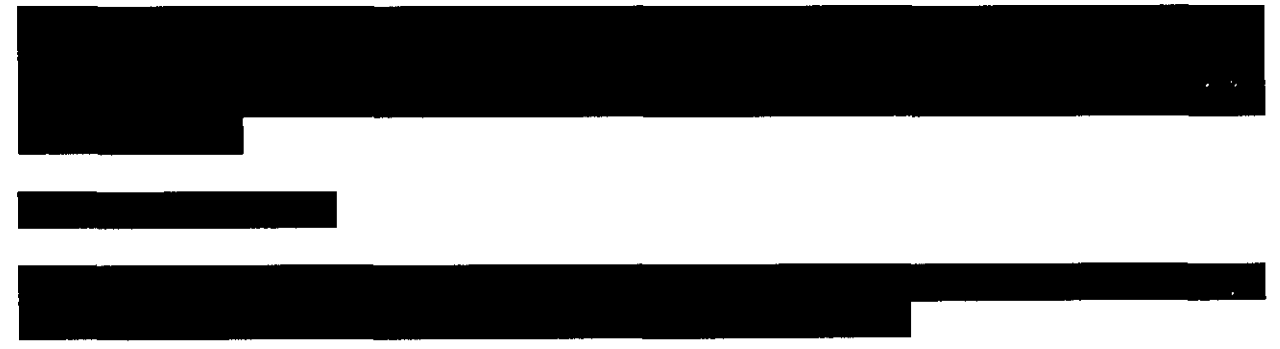
6.1 AT&T

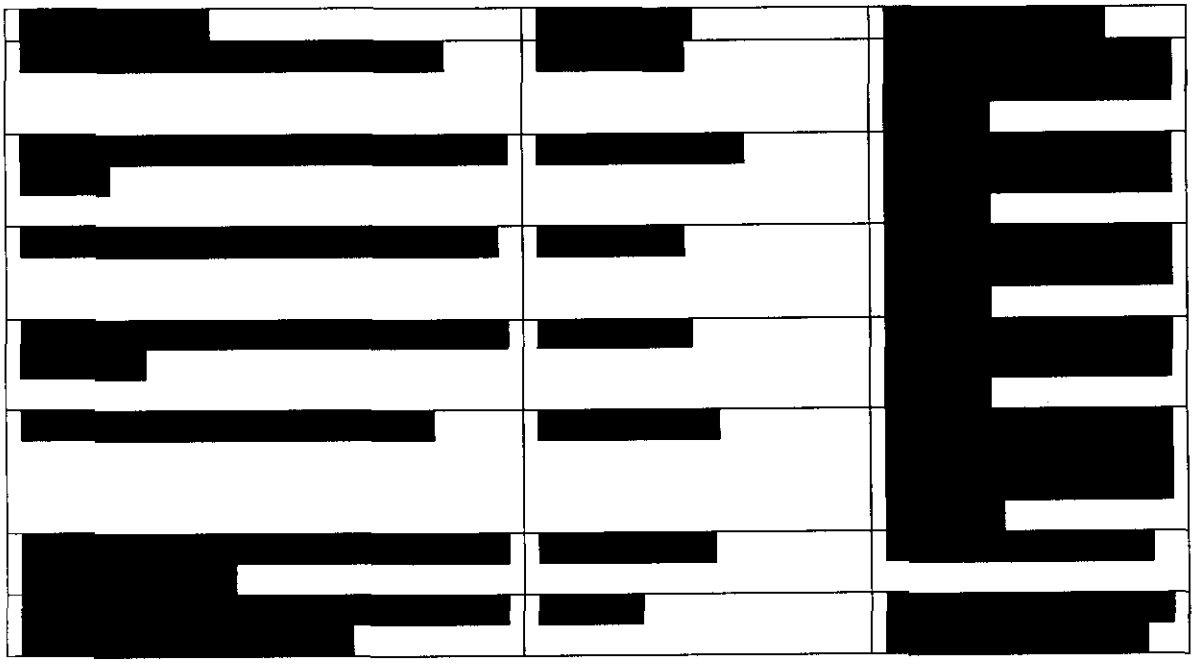
To be determined.

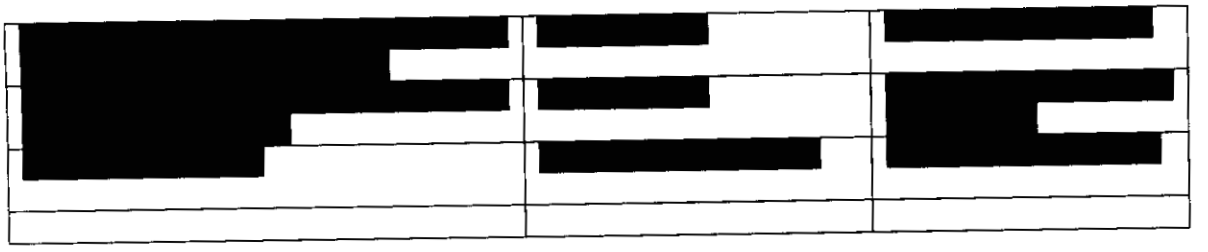
6.2 Embarq

To be determined.

6.3 Verizon







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)			[redacted]
Proactive data security programs (IT and Customer Service)			[redacted]
Audit of IT / Customer Data operations in the last 24 months			[redacted]
Number of security breaches, last 24 months			[redacted]
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)			[redacted]
Total number of employees			[redacted]
Number of employees with access to customers' social security numbers			[redacted]
Work-at-home program for Customer Service Representatives			[redacted]
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:

[redacted]