M|C
&|S
MESSER CAPARELLO & SELF, P.A.
Attorneys At Law
www.lawfla.com

December 17, 2007

RECEIVED-FPSC
07 DEC 17 PM 4:20
COMMISSION CLERK

BY HAND DELIVERY
Ms. Ann Cole, Director
Commission Clerk and Administrative Services
Room 110, Easley Building
Florida Public Service Commission
2540 Shumard Oak Blvd.
Tallahassee, Florida 32399-0850

REDACTED

080063-EI

Re: Undocketed; Request for Confidential Treatment of Portions of the Staff Report Entitled "Customer Data Security of Florida's Five Investor-Owned Utilities" by Florida Public Utilities Company

Dear Ms. Cole:

Enclosed for filing on behalf of Florida Public Utilities Company are an original and 15 copies of a Revised Request for Confidential Treatment in the undocketed matter referenced above.

Please acknowledge receipt of these documents by stamping the extra copy of this letter "filed" and returning the same to me.

Thank you for your assistance in this matter.

Sincerely,

Norman H. Horton, Jr.

CMP ____
COM ____
CTR ____
ECR 1
GCL 1
OPC ____
RCA ____
SCR ____
SGA ____
SEC ____
OTH 1 conf records

NHH:amb
Enclosures
cc: Ms. Julie Petty

(See DN 10847-07 Conf.)

DOCUMENT NUMBER-DATE
10986 DEC 17 07
FPSC-COMMISSION CLERK

Regional Center Office Park / 2618 Centennial Place / Tallahassee, Florida 32308
Mailing Address: P.O. Box 15579 / Tallahassee, Florida 32317
Main Telephone: (850) 222-0720 / *Fax:* (850) 224-4359

REDACTED

BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

In re: Request for Confidential Treatment of portions of the Staff Report entitled "Customer Data Security of Florida's Five Investor-Owned Utilities" by Florida Public Utilities Company	)))))	080063-EI ~~Undocketed.~~ Filed: December 17, 2007

FLORIDA PUBLIC UTILITIES COMPANY'S
REVISED REQUEST FOR CONFIDENTIAL TREATMENT

COMES NOW, Florida Public Utilities Company ("FPUC" or "Company"), through its undersigned and files this Revised Request for Confidential Treatment of portions of the Staff Report entitled "Customer Data Security of Florida's Five Investor-Owned Utilities." As basis, the Company states:

1. On December 11, 2007, FPUC filed a Request for Confidential Treatment of Portions of the draft report of the policies, practices and controls regarding security of sensitive customer information for each of the electric IOUs, including FPUC. Upon review of the request filed December 10, 2007, FPUC herewith submits the revised request.

2. In the Draft Report, Staff summarizes and discusses the policies and procedures of the Company based on interviews and data responses provided by the Company. The Draft Report also includes comments and conclusions of Staff regarding these measures. While such commentary may be helpful to the Commission, a public discussion and disclosure of this type of information could assist unauthorized access to sensitive information and cause harm to both the

Company and its customers. Accordingly, FPUC is requesting confidential treatment of portions of the draft report and Staff workpapers.

3. Section 366.093, Florida Statutes, permits electric utilities to request certain records and material be kept confidential and exempt from Section 119.07(1). Among the information which is included as proprietary and confidential are security measures, systems or procedures. (Section 366.093(3)(c), Florida Statutes). The draft report contains discussions of this type of information but more importantly analysis and conclusions regarding these systems and procedures. FPUC does not publish or make public reviews and conclusions regarding the overall effectiveness or recommendations of its various policies and procedures nor does it intend to do so. Accordingly, FPUC would request that the portions of the draft report and Staff workpapers identified on Attachment "A" hereto be determined to constitute proprietary confidential business information regarding security measures, systems or procedures encompassed within Section 366.093(3)(c) and exempt from Section 119.07(1).

4. References to pages are to the document which accompanied the November 16, 2007, letter.

5. Exhibit "A" hereto in a sealed envelope is a copy of the draft report and workpapers with the information which FPUC asserts is confidential highlighted. Exhibit "B" hereto is a copy of the draft report and workpapers that have been redacted.

6. This Revised Request is intended to revise the scope of the information for which confidential treatment is being sought and requests return of the initial request.

7. The Company makes this request with reference to the material in the draft report but would include this request as to the final report as well.

Respectfully submitted,
MESSER, CAPARELLO & SELF, P. A.
Post Office Box 15579
Tallahassee, FL 32317
(850) 222-0720

NORMAN H. HORTON, JR., ESQ.

Attorneys for Florida Public Utilities Company

ATTACHMENT "A"

Identification	Reason
Page 7, Exhibit 1, "Customer Data Security Issue Summary" all items in column headed "FPU"	366.093(3)(c)
Page 8, paragraph 1.42, handwritten numbered lines 1-6	366.093(3)(c)
Page 33, all or part of handwritten numbered lines 1-4	366.093(3)(c)
Page 34, handwritten numbered lines 1-12; all or part of 13-14	366.093(3)(c)
Page 35, all or part of handwritten numbered lines 1-3 16-32	366.093(3)(c)
Page 36, all or part of handwritten numbered lines 1-2 and 8-9	366.093(3)(c)
Pages 39, all or part of handwritten numbered lines all or part of 2-9	366.093(3)(c)
Page 40, all lines	366.093(3)(c)
Staff workpapers "Interview Summaries" tab paragraph (3) conclusions, entire section	366.093(3)(c)

COMMISSIONERS:
LISA POLAK EDGAR, CHAIRMAN
MATTHEW M. CARTER II
KATRINA J. MCMURRIAN
NANCY ARGENZIANO
NATHAN A. SKOP

STATE OF FLORIDA

DIVISION OF COMPETITIVE MARKETS & ENFORCEMENT
BETH W. SALAK
DIRECTOR
(850) 413-6600

Public Service Commission

November 16, 2007

Ms. Julie Petty
Director, Customer Relations
Florida Public Utilities Company
401 South Dixie Highway
West Palm Beach, Florida 33402-3395

Dear Ms. Petty:

Enclosed is a draft copy of our report entitled ***Customer Data Security of Florida's Five Investor-Owned Utilities.*** This draft includes the Executive Summary, Background & Perspective, the Florida Public Utilities Company chapter, and three appendices. The review examined the data security practices for each of Florida's five-investor owned utilities. It is our hope that each company finds this assessment beneficial.

This draft is provided for review of factual accuracy and identification of any material on which you intend to file a request for confidential classification. You have the right to file a request in accordance with *Rule 25-22.006(3), F.A.C.* The request must be filed with the Division of the Commission Clerk and Administrative Services no later than 21 days from the date of receipt, or we retain the right to publish without regard to confidentiality. During the next 21 days, staff will be available to discuss the factual accuracy of the report and to provide access to work papers for review of prospective confidential information. Also during this period, staff will accept any written comments the company may want to include in the final report.

We would like to publish the report as soon as possible after the 21 day period for filing expires on **December 11, 2006**. Thank you for your cooperation and assistance, and that extended by Florida Public Utilities Company employees who participated in this review. If you have any questions, please contact **David Rich** at (850) 413-6830.

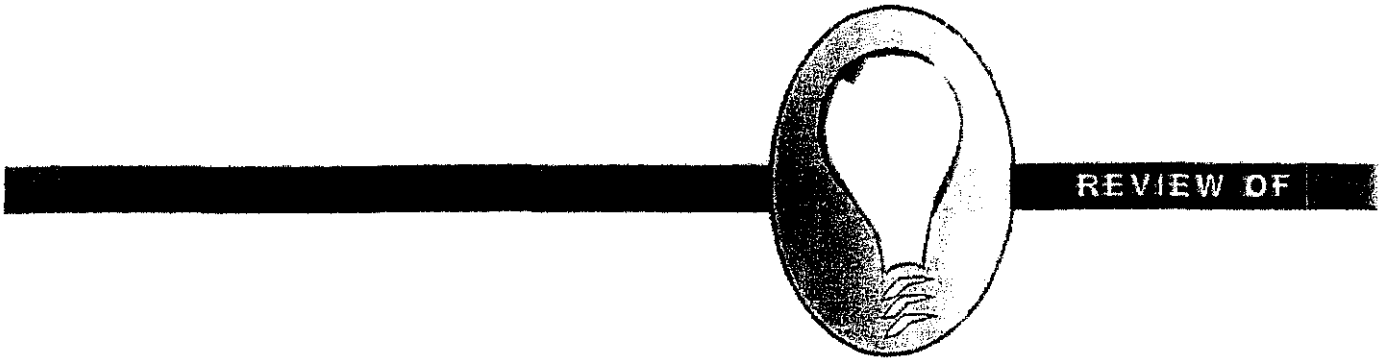
Sincerely,

Lisa S. Harvey
Bureau Chief

cc: Beth Salak, Director, Division of Competitive Markets and Enforcement
Dale Mailhot, Assistant Director, Division of Competitive Markets and Enforcement

EXHIBIT "A"

NOVEMBER 2007



Customer Data Security

OF

Florida's Five Investor-Owned Electric Utilities

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

Review of
Customer Data Security
of
Florida's Five Investor-Owned Electric Utilities

William "Tripp" Coston
Project Manager,
Operations Review Specialist

David F. Rich
Operations Review Specialist

November 2007

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

PA-07-05-005

TABLE OF CONTENTS

1.0 Executive Summary

1.1 Objectives

This review of Florida's investor-owned electric utilities 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 learn more about each company's policies, practices, and controls regarding the security of sensitive customer information.

The primary objectives of this review were:

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

1.2 Scope

The review focused on examining each company's procedures, processes, network systems, and operational controls for safeguarding sensitive customer data. Staff reviewed information technology (IT) 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, and
- Audits of Data Security.

1.3 Methodology

The five investor-owned utilities were each reviewed separately. During the review, staff gathered information from each company through document requests. After careful study of the responses from the document requests, staff conducted on-site interviews with each company. Key company employees in the functional areas were interviewed. The review was conducted between June and October 2007.

Each company's policies, practices, and procedures were compared to applicable state and federal statutes relevant to the protection of sensitive customer data. Staff made comparisons to relevant standards such as those shown in **APPENDIX A**. Staff also reviewed the current physical and virtual security systems used by each company, those now being implemented, and concepts in stages of either planning or development.

To assess and compare companies' overall security posture, staff used the information gathered from the document reviews, on-site interviews, and facility visits to assess each company's overall security status.

1.4 Overall Opinion

All of the companies are in compliance with applicable state and federal statutes and industry guidelines for security of sensitive customer information.

Each company recognizes the integral role management has in establishing an overall corporate climate conducive to safeguarding customer information. Management in each investor-owned utility has tailored company goals and objectives, policies, programs, and procedures to respond to their particular information security environment and perceived risk.

No company reported, or is aware of, any breaches to 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 and continued vigilance is required.

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, this is indicated in the chart by a solid circle (●) symbol. Where a deficiency was noted, this is indicated in the chart by an open circle (○) symbol. The Control Elements within Management Oversight, IT Controls, User Awareness, Outsourcing Controls, and Auditing Controls are individually discussed in more detail in chapters three through seven.

Customer Data Security Issue Summary

MANAGEMENT OVERSIGHT					
CONTROL ELEMENTS	FPL	FPU	GULF	PROGRESS	TEC
Clearly understands that information security is a management responsibility		[redacted]			
Personal information is collected					
Assesses the appropriateness of the information collected from customers					
Adequately limits the use and disclosure of customer's personal information					
Access to customer information from remote locations					
Controls for remote access to customer information					
[redacted]					
[redacted]	FPL	FPU	GULF	PROGRESS	TEC
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					
Management routinely monitors and assesses system security					
[redacted]					
	FPL	FPU	GULF	PROGRESS	TEC
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					
[redacted]					
	FPL	FPU	GULF	PROGRESS	TEC
Access to customer information provided to third parties					
Controls are in place to prevent disclosure of customer information by third parties					
[redacted]					
	FPL	FPU	GULF	PROGRESS	TEC
Access to competent data security auditing resources exist					
Data security is periodically assessed					
Information security breaches are reported to appropriate management					

● No Issue ○ Issue

EXHIBIT 1

Source: Company Data requests 1 and 2

Staff's findings for each company are summarized below. Additional discussion of staff's conclusions for each company is contained in chapters three through seven. A profile of company data security information is provided in **APPENDIX B**. A company-by-company recap of the treatment of sensitive customer data is provided in **APPENDIX C**.

1.4.1 Florida Power & Light (FP&L)

[redacted]

1.4.2 Florida Public Utilities Company (FPU)

With significantly fewer customers, employees, and other assets at its disposal, FPU's depth and breadth of measures to safeguard sensitive customer information are not as robust as those of other Florida investor-owned utilities. However, staff believes that FPU has generally adequate safeguards in place to protect this information and that company management has assessed risk, allocating assets as required to meet threats. The company is in compliance with state, federal, and industry guidelines relevant to protecting sensitive customer information.

1.4.3 Gulf Power Company (Gulf Power)

1.4.4 Progress Energy Florida (PEF)

1.4.5 Tampa Electric Company (TEC)

2.0 Background and Perspective

The social security number is one of the most valuable bits of information needed to commit identity fraud. The social security number has evolved from a tracking number used by the government's retirement system to a personal identification number used by such entities as the Internal Revenue Service and Credit Reporting Agencies. This evolution of the social security number has created a greater need to protect and secure its use and exposure. While the social security number is the most critical component for identity theft, other information such as date of birth, driver's license number, address, phone number, and credit card account numbers can also be useful in facilitating identity theft.

Each individual bears the responsibility to be judicious in securing his personal information. Many times, identity theft occurs when a victim loses his information or carelessly exposes the information to opportunistic thieves. However, there are times when consumers must entrust personal information to a business or agency. Therefore, there is an expectation that reputable companies, such as utilities and financial institutions, will earnestly protect this sensitive information.

2.1 Federal Trade Commission Role

In 1998, the Federal government enacted the Identity Theft and Assumption Deterrence Act which made it a violation of federal law to intentionally misuse someone's identifying information or existing accounts, or to establish an account in his name.[1] The act charged the Federal Trade Commission (FTC) as the federal governmental agency that works to protect consumers from identity theft. Citizens who are victims of identity theft can report the crime to the FTC, and the FTC is charged with collecting complaints from victims and sharing the information with necessary federal, state, and local law enforcement.

In 2003, the FTC sponsored a survey on the topic of identity theft. The results support the concerns of many Floridians: identity theft is a real threat; protecting one's personal information is critical. 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 *2003 FTC Identity Theft Survey Report* indicated that during the previous 12 months, 4.6 percent of the population experienced some type of identity theft. In the previous five years, 12.7 percent (approximately 27 million citizens) reported being victims of some type of identity theft. The report shows that identity theft impacted 9.91 million citizens in the previous 12 months at a cost of $52.6 billion. The report also states that, on average, it takes a victim 30 hours of work to resolve the impacts of identity theft; with up to 60 hours expended in situations where a new account is fraudulently established.[2]

---

[1] Public Law 105-318, 112 Stat 3007 (October 30, 1998)
[2] *2003 FTC Identity Theft Survey Report*

The FTC tracks complaints annually by type and location. In 2006, Florida ranked fifth in the nation (cases per 100,000), with 17,780 reported victims. The Miami Fort Lauderdale Metropolitan Statistical Area had the largest number of Florida complainants in 2006, at 7,557.[3] The total number of reported victims within the state has increased each year, with 12,816 in 2002; 14,119 in 2003; 16,062 in 2004; and 17,048 in 2005.[4] These numbers only represent the number of victims who notified the FTC of the crime, rather than the actual total number of victims during the period. The 2003 FTC study notes that only 25 percent of the participants reported the crime to local police, and only 22 percent notified a credit agency.[5]

The FTC categorizes complaints based on how the victims' information was misused, including phone or utility fraud. Of note, the 2006 Florida data indicates that approximately 4.7 percent of complainants reported unauthorized establishment of new (non-telecommunications) utility accounts. This has increased from a low of 3.3 percent in 2003.[6]

2.2 Data Security Breaches

One of the most publicized breaches occurred in 2005, when 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 as their business address. ChoicePoint not only ignored red flags, but used unsecured fax machines for correspondences.[7]

Also in 2005, Bank of America admitted to losing a back-up file that held 1.2 million customers' personal information. In the same year, Bank of America, Wachovia, Commerce Bancorp, and PNC Financial Services Group detected illegal sales of account information by bank employees. 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."[8]

2.2.1 Recent Florida Breaches

Companies operating within Florida are not immune to unintentional exposure or intentional breaches of customer information. The following list highlights several recent events in which customer information was exposed through unauthorized events.[9]

- In March 2005, Customer records of a Florida-based subsidiary of the LexisNexis Group were compromised when hackers used malicious programs to collect valid

[3] Figure 7a – 2006 national complaint data
[4] *2002 – 2005 national complaint data*
[5] *2003 FTC Identity Theft Survey Report*
[6] 2003-2006 Figure 2, Complaint data-Florida
[7] *ChoicePoint Settles Data Security Breach Charges, to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006. Retrieved July 11, 2007. www.ftc.gov/opa/2006/01/choicepoint.shtm
[8] *Bank Security breach may be bigger ever*, May 23, 2005. Retrieved July 2007. www.Money.cnn.com
[9] Compiled from Privacy Rights Clearinghouse Chronology of Data Breaches. Updated through Aug. 7, 2007. Retrieved August 9, 2007. www.privacyrights.org/ar/ChronDataBreaches.htm

customer ID passwords and to 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, in 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 of its members, including names, social security numbers, dates of birth, and mother's 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 on approximately 12,000 adoptive and foster-parents.

- In June 2007, Jacksonville Federal Credit Union realized that social security numbers 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 2,300,000 customer records were stolen by a worker from one of the company's subsidiaries. The information stolen included credit card and bank account numbers, and other personal information.

2.2.2 Potential of Exposure

The Privacy Rights Clearinghouse, a non-profit consumer information and advocacy organization, annually compiles a listing of all data breaches.[19] In review of the cases reported between 2005 to present, the majority of breaches can be categorized into four basic groups: technology, online exposure, insiders, and improper storage or disposal of customer records.

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

Online exposure can include personal information that is inadvertently loaded onto the internet. Search engines, such as Google, can pick-up names through company Web sites and expose the information through the World Wide Web. Also, e-mails that include personal information may be sent to the incorrect addressee. Unencrypted e-mails may also be intercepted by hackers or malicious software.

[19] www.privacyrights.org/ar/ChronDataBreaches.htm

Insiders can be either dishonest employees whose intent is to commit fraud, or a well-intentioned employee who may commit an error in judgment. A dishonest employee can 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 allow employees to collect and store data. This could include well-intentioned employees who take personal information off-site for work-related needs, but have the information stolen or lost while away from the office.

Improper storage or disposal can be an easy target for thieves looking for easy access to someone's personal information. This can include not only paper files that are left exposed, un-shredded, stolen, or improperly disposed, but also electronic files that are not maintained accordingly. Also, mailings that include exposed sensitive information could lead to a breach of information. Finally, disposal of discontinued office equipment could lead to a breach if electronic hard drives and memory devices are not properly "cleaned" prior to discarding the device.

2.3 Federal and State Authority

Several State and Federal statutes and initiatives govern data security and identify theft. These apply either directly or indirectly to Florida's electric utilities and should be considered in developing security practices and procedures.

2.3.1 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 mask 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.

The disposal requirements instruct businesses to properly dispose of documents containing customer information. Proper disposal includes burning or shredding of paper reports and erasing electronic storage devices. It can also include contracting the service out to a qualified disposal company.

2.3.2 Fair Debt Collections Privacy Act

This act limits the information that a creditor, or its agent, can provide to a third-party. It prevents a creditor, or its agent, from disclosing to a third-party that an individual is in debt. This law would prevent a utility from disclosing any past-due or charge-off information to any other than the customer of record or authorized user.

2.3.3 Florida Statute 817.568 and 817.5681

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

2.3.4 Presidential Task Force of Identification Theft

In May 2006, President George W. Bush issued an Executive Order 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."[11] The task force's April 2007 strategic plan recognizes 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."[12] The task force has recommended the development of a comprehensive record on private sector use of social security numbers, including evaluating their necessity. The Task Force will make its recommendations by the first quarter of 2008. Until future recommendations are made, there are current federal and state laws in place that recognize and enforce the importance of safeguarding customer sensitive information.

2.4 Florida Public Service Commission Responsibility

Chapter 350.117 allows the Commission to conduct management and operation audits for any regulated company to ensure adequate operating controls exist. This report addresses whether each of the five companies audited for customer data security have proper controls in place. The audit particularly focused on management controls, information technology controls, user awareness, outsourcing controls, and auditing. Each of the following company chapters addresses these controls in a question and answer format.

[11] President's Task Force Strategic Plan p. viii
[12] President's Task Force Strategic Plan p. 24

4.0 Florida Public Utilities

The two divisions of Florida Public Utilities Company (FPU) have 346 full-time and 6 part-time employees, and serves approximately 28,000 electric customers in Florida. The Northwest Division, headquartered in Marianna, provides service to customers in the western panhandle. The Northeast Division serves Amelia Island and is located in Fernandina Beach.

4.1 Management Oversight

Does Florida Public Utilities management have a clear understanding that information security is a management responsibility?

FPU management acknowledges that information security is a management responsibility. According to FPU, company management sets the corporate climate for information security by creating procedures and determining information security priorities.

FPU management states that it recognizes that information security is only possible, and produces the best results, in a cooperative partnership with company employees. Further, the company states its objective relevant to information security is to create and sustain a workforce aware of the obligation to effectively manage and protect sensitive customer information. FPU managers stated that the company seeks to accomplish this objective through a comprehensive employee training program, management supervision of the workplace, employee mentoring, retraining (when necessary), and annually requiring all employees to acknowledge and sign the "Security of Customer Data" policy statement.

According to the company, managers and supervisors also routinely monitor software applications, programs, workstations and employee access to sensitive information to determine inherent operational risk. Changes in employment status, or an employee's business need to access sensitive customer data, are reported by managers to IT. Then, the employee's network access rights are revised to reflect the change, minimizing risk.

What type of personal information does Florida Public Utilities collect from customers?

The Customer Information System (CIS), a customer service and billing system, is used to initiate new accounts, update record information, and to store individual customer data. When initiating a new residential account, customer service representatives (CSRs) collect personal information from the account holder including the full name, social security account number, driver's license number, address, and phone number.

FPU service representatives also collect banking information if the customer wishes to establish automatic electronic payments. During initiation, customers also have the opportunity to provide names of others authorized to discuss the account, such as a spouse or other relative.

Has Florida Public Utilities management assessed the appropriateness of the information collected from customers?

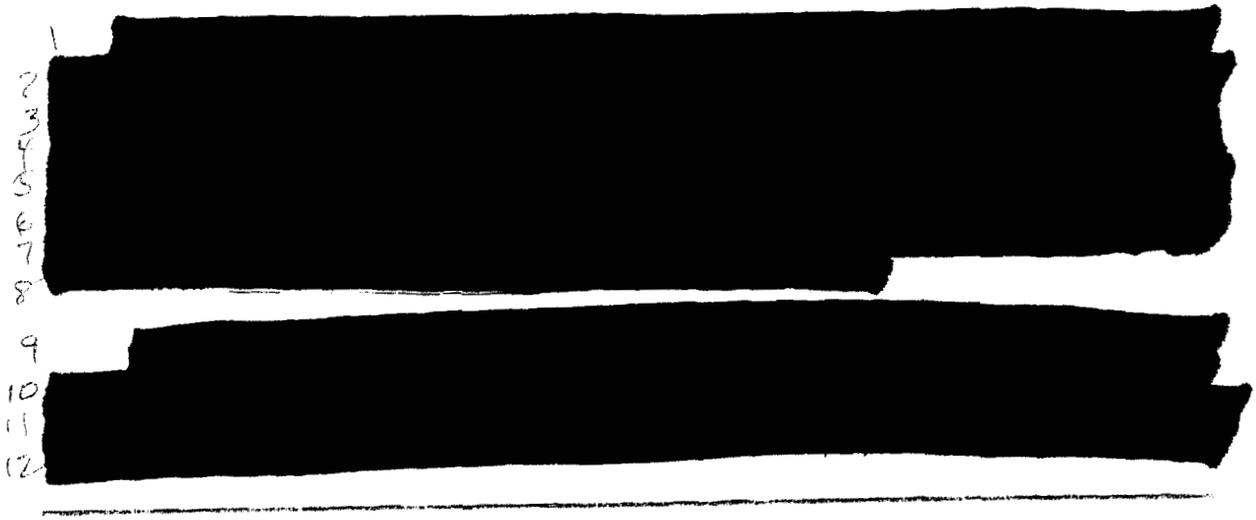
FPU routinely collects both a social security number and driver's license number from a majority of its customers. According to the company, a social security number is required in order to run a credit worthiness check. Thereafter, the social security number is maintained for identification purposes and possible future collection actions.

The company reported that new customers are increasingly wary of identity theft and often do not wish to provide a social security number. In such cases, the driver's license number can be used as an alternative method of identification and to assist in possible future collections action. The driver's license information is maintained for the life of the account, all but the last four digits are masked, and FPU management does not perceive any undue risk in collecting or keeping this information.

Staff believes that requiring a driver's license number for identification purposes in the absence of a social security number may be appropriate. But, in the event that a social security number is obtained for identification and credit check, the additional need for collecting and maintaining driver's license information is not apparent. Staff believes that collecting any personal information beyond that which is absolutely needed poses unnecessary risk.

Does Florida Public Utilities adequately limit the use and disclosure of customers' personal information?

FPU has operational practices for customer service personnel to follow that address the use, disclosure, and retention of sensitive customer data. FPU has 32 customer service representatives, 4 customer service supervisors, and 5 customer service managers to initiate new accounts and respond to other customer inquiries. Corporate headquarters is in West Palm Beach, but all payment processing is done in the Marianna office. The Director of Customer Relations supervises the billing of customers in both divisions.



Service Manager and General Manager of the Northeast division, the Customer Service Manager and General Manager of the Northwest division, the Director of Customer Relations, and the Customer Information Manager. Customer Service Managers or General Managers make an information request to either the Director of Customer Relations or Customer Information Manager who is able to query the database. The "legitimate business need" for such information is determined informally.

FPU procedures prohibit discussing confidential customer information with anyone other than the account holder, unless the requestor was previously authorized by the account holder. This restriction also applies to walk-up or telephone inquiries. When a non-account holder inquires, the CSR asks the individual for his or her name. For walk-ins, CSRs confirm pre-existing authorization and then view personal identification, such as a joint checking account or driver's license, prior to discussing an account. On the phone, CSRs ask for a name and then request additional confirmation. [redacted] Most account holders establish an authorized third party during account initiation. However, CSRs do not normally ask new customers whether they wish to establish another authorized user.

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

FPU managers stated that the company recognizes the inherent data security risk associated with any employees remotely accessing the network. Each Division General Manager and Operations Manager has remote access authorization to those portions of the network containing sensitive customer information. Nine IT employees also have the capability to access the network remotely. The company stated that it believes proper controls are in place to appropriately limit access.

What controls have Florida Public Utilities put in place for remote access of customer personal information?

Under normal operating conditions, remote access is limited to Division General Managers and Operations Managers. FPU does not allow customer service representatives to remotely access the network and has no work-from-home program. Management stated there is no current or anticipated need to undertake such a program. FPU has a post-hurricane contingency plan which would allow CSRs remote access if normal operations were rendered impossible due to extensive damage to company offices. [redacted] The virtual private network, or VPN, connects to a secure concentrator at the corporate office.

4.2 Information Technology Controls

Has Florida Public Utilities established an appropriate data security management function?

FPU's Director of Information Technology directly reports to the President & CEO. The IT Director has nine employees working in the information technology division.

According to FPU management, information management and security are the responsibility of all FPU personnel. FPU's Information Management (IM) section is specifically designated with the responsibility to assess the risks and potential vulnerabilities to the overall network and individual workstations. IM managers coordinate with, and provide technical advice to, company operational management in order to determine FPU policy, practices, and procedures relative to the handling, retention, and protection of sensitive customer data.

IM personnel also have the responsibility to monitor employee access to the network, its functions, and stored information. System usage is monitored, and the IM section processes all changes to employee network access. A change in employment status, such as retirement, termination, promotion, or transfer prompts an immediate review of access and any appropriate changes to authorization.

Has Florida Public Utilities established appropriate information security policies, procedures, and guidelines?

FPU information technology employees seek to establish appropriate information security policies, procedures, and guidelines in a variety of ways. These include:

[redacted]

Information Management employees also 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 to enhance programs. [redacted] Only software patches produced by authorized

vendors are used. [redacted] As a further precaution, no patch is installed until it has been first tested to ensure its compatibility with current network configurations and will not harm existing programs or data.

Operational managers coordinate with information management throughout each phase of the patch process. They receive testing results, evaluate the effects, and assess risk for each patch prior to full uploading on the existing network. Only company management can authorize a system-wide installation of patches based on test evaluation and risk assessments.

FPU information management is planning two significant improvements directly linked to information security. The first is an upgrade to existing Cisco wireless access devices to the next level of available security. Second, the company will be raising security certificates to the 128-bit encryption level.

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

According to FPU management, information security is not possible without parallel security of the Information Management (IM) parent site located in West Palm Beach. Access to this facility is controlled by a magnetic lock. [redacted]

Does Florida Public Utilities restrict access to customer information related software functions, data, and programs?

The company network has many levels of resident security. All users must have a valid user name and password. Access is authorized based on a business need-to-know and contingent on approval by both supervisors and information management. Access to different parts of the network is derived from a menu at each workstation, tailored to individual users. Lack of the appropriate level of access authority will result in denied access. Different programmers have either very wide or universal network access, but are subject to continual monitoring.

[redacted] The *Global Technology Audit Guide (GTAG)* establishes best practices for information security, derived from industry sources worldwide. These practices support effective information security management and, when used, significantly reduce the risk of compromise. A key component of these practices is employing a defense in depth, a system of active and passive measures to thwart network compromise. The premise of defense in depth is to layer physical and virtual security, combining passive intrusion detection systems and active intrusion prevention systems. [redacted]

Does Florida Public Utilities monitor software security activity and produce appropriate management reports?

FPU information management has the ability to monitor employee access to the network and sensitive information in real time. This oversight provides IM 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.

The information management system automatically monitors and captures software and access activity around the clock. The results are available for regular review by IM personnel. Network information is then routinely made available to management in the form of two reports, the *Access Report* and the *Use Report*. These are also available on very short notice through a request to IM. The *Access Report* pinpoints who within FPU has current access authority for all network functionalities, while the *Use Report* documents employee usage on the network, sites visited, and e-mails.

4.3 User Awareness and Training

Does Florida Public Utilities have adequate privacy and data security policies and procedures?

Annually, FPU policy requires all employees to read and acknowledge by signature the *Florida Public Utilities Code of Ethics*, dated February 2005 and the *Employee Conduct and Work Rules*. However, the *Florida Public Utilities Code of Ethics* only briefly addresses the

handling of sensitive customer information and does not site specific laws or regulations. Due to the relatively small size of FPU, all signed copies for 2007 from Marianna Division employees were verified. The *Employee Conduct and Work Rules* policy defines unauthorized disclosure of confidential information as sufficient for disciplinary action. The *Computer, E-mail, Voice Mail, and Internet Use* policy outlines proper use of these functionalities, but does not address customer sensitive data specifically.

Though these policies do not specifically focus on the protection of sensitive customer information, FPU management states that it believes each policy helps create an employee mindset that is conducive to safeguarding customer sensitive data, and transferable to the application of such safeguards.

Security of Customer Data is a specific data security policy and procedure requiring full understanding and acceptance by all employees. New employees must read and acknowledge the policy by signature upon completion of initial training and annually thereafter.

Are Florida Public Utilities employees properly trained on privacy and data security policies?

According to the company, an expectation of ethical behavior regarding the handling of sensitive customer information is incorporated into the FPU training program. FPU provides formal initial training for all new employees using a combination of written policies, established practices, and standardized procedures pertaining to the security of sensitive customer information. As a part of this training, each employee is required to read and sign the *Security of Customer Data* policy and procedure notice.

Trainers from the West Palm Beach headquarters visit the divisions up to four times annually, conducting refresher training for all employees. According to FPU, there are always customer service and data security components to this training. On-the-job training is used to augment the initial training of new customer service representatives. A new customer service representative first shadows a more senior employee and, later, the roles are reversed. When the new employee demonstrates a thorough knowledge of correct customer procedures and data safeguards, he or she is allowed to work without direct, constant supervision. Every supervisor and manager attended supervisory training in May of 2007. The training was conducted by the corporate attorney and included instruction on company policies pertaining to privacy, data security, and ethics.

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

Florida Public Utilities' *Progressive Disciplinary Procedure* policy establishes a formal five-step disciplinary process which escalates in severity from a first (verbal warning) to fifth step (termination). At the lower end of the severity scale, FPU commonly combines mentoring and retraining verbal or written warnings to redress conduct violations. Depending on the nature and severity of the misconduct, the process can be accelerated.

4.4 Outsourcing Controls

Does Florida Public Utilities provide third parties with access to customer personal and / or banking information?

Florida Public Utilities does not outsource customer services. The CIS billing vendor with which FPU has a service/support agreement has access to customer records in CIS in order to diagnose and correct billing-related errors. The only other outside vendor with access to customer information is the company auditors.

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

FPU uses confidentiality clauses whenever contracting for third party audit or repair service and support. These clauses require the third party to adhere to FPU protocols, policies, and procedures regarding sensitive customer information. Company management believes the current confidentiality agreements, in contracts between FPU and outside firms, adequately safeguards customer information.

[redacted]

FPU states that it further limits the risk of personal information disclosure by choosing not to use satellite company payment locations or authorized third party payment stations.

4.5 Auditing Controls

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

FPU does not employ full time staff auditors. The auditing firm of Binder, Dijker, Otte & Company (BDO) is the external auditor for FPU. BDO, an international accounting firm, was founded in Europe in 1963. US offices were established in 1988. BDO's auditing expertise is in finance and accounting. BDO conducted a financial audit annually for FPU during the two year period covered by this review. Binder, Dijker, Otte & Company audits do not focus specifically

on information technology or information security. However, FPU stated that the BDO audit findings still provide general insights on data security and network protection.

Crowe Chezik is the FPU internal auditor. Founded in 1942, Crowe Chezik is one of the top ten public accounting and auditing firms in the nation.

Does Florida Public Utilities periodically assess the organization's information security practices?

No audit of FPU information security practices was performed over the period 2005 to September, 2007. However, FPU has recently initiated an audit of network security and risk assessment by Crowe Chezik, their internal auditors. The audit will focus on Sarbanes-Oxley IT controls. Completion of the audit is anticipated in October 2007.

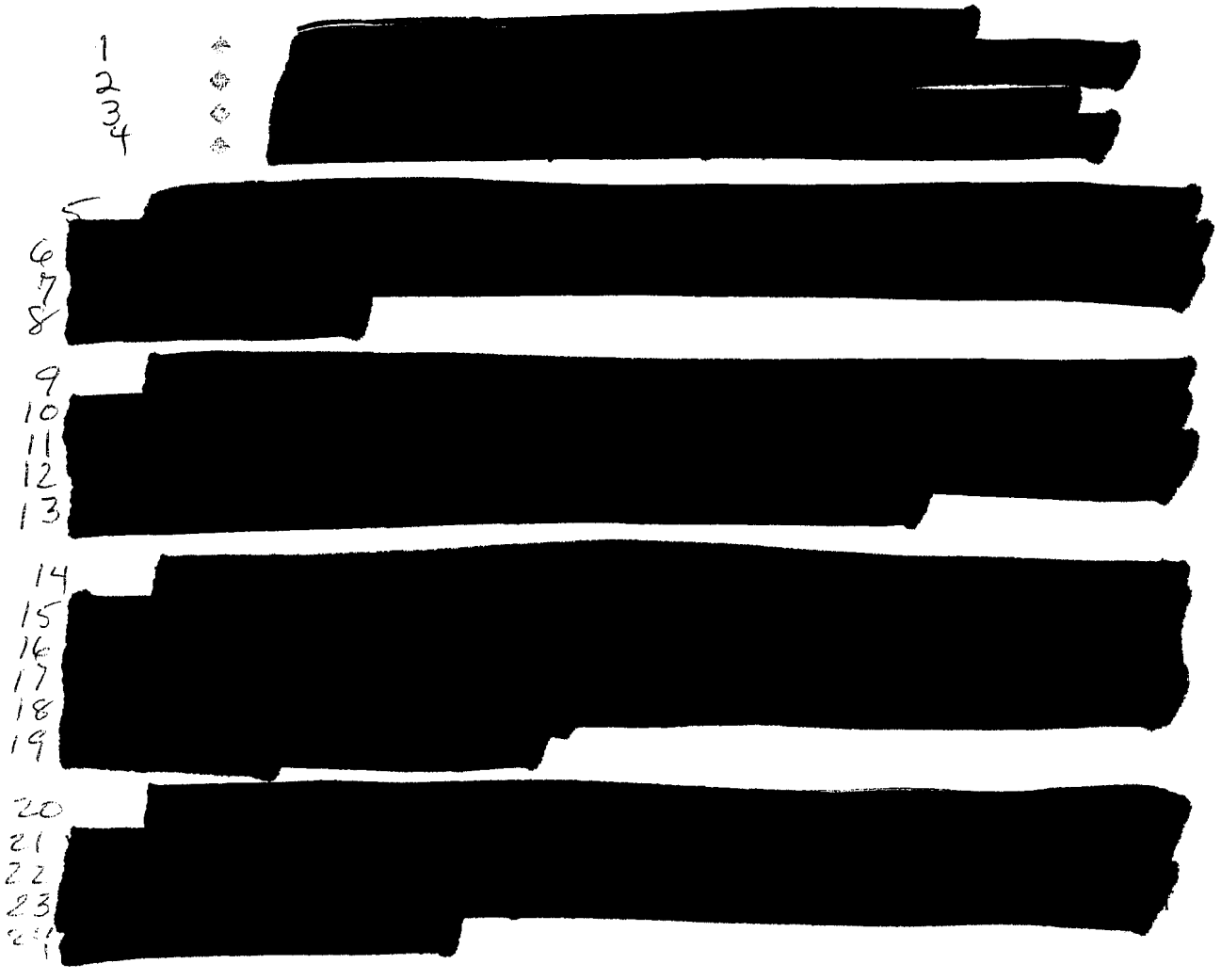
Has management provided assurance that information security breaches, and conditions that might represent a threat to the organization, will be promptly made known to appropriate Florida Public Utilities' corporate and IT management?

Florida Public Utilities has no internal audit department. Matters relating to information management are the responsibility of management and IT personnel. In the event of any breach or compromise to sensitive customer data, the incident and pertinent facts surrounding it are required by company policy to be reported to both.

Management stated that there have been no detected incidents of internal or external sensitive information compromise during the last two years. According to the company, there has not been a single theft or loss of data, disks or other storage media, laptops, or an external compromise of any sort to the network.

4.6 Conclusions

With significantly fewer customers, employees, and other assets at its disposal, FPU's depth and breadth of measures to safeguard sensitive customer information [redacted]



APPENDIX A

GLOBAL TECHNOLOGY AUDIT GUIDE (GTAG)

GTAG's privacy best practices are derived from a variety of worldwide sources and were central to staff's review. These privacy best practices support prudent data security management and reduce risk for those companies that routinely use these techniques as part of their overall corporate plan. The privacy best practices considered during this review include:[13]

- Performing adequate and regular privacy risk assessment;
- Establishing a privacy officer or organization to serve as the focal point for coordination of privacy activities and the handling of complaints or issues;
- Developing awareness around key data handling and identity theft risks;
- Masking personal identification numbers, such as social security numbers, and other sensitive information when possible;
- Supervising and training call center staff to prevent social engineering and similar risks;
- Managing marketing lists and all third-party vendor relationships effectively;
- Creating awareness of Web and e-mail vulnerabilities;
- Developing record retention and destruction policies;
- Implementing a data classification scheme based on the sensitivity and data mapping;
- Conducting risk assessments of access controls, physical security access restrictions, and change controls;
- Implementing intrusion detection and prevention technologies;
- Completing penetration testing and independent testing/review of key controls systems, and procedures; and
- Limiting data collection to operationally necessary data.

[13] Global Technology Audit Guide, "Managing and Auditing Privacy Risks." The Institute of Internal Auditors. p. 15-16, June 2006

APPENDIX B

CUSTOMER DATA SECURITY INFORMATION

Florida investor-owned utilities have programs designed to safeguard sensitive customer information. These programs are multifaceted, combining written policies, employee procedures, and management or supervisory practices. A variety of virtual and physical safeguards round out the data security system found in each company.

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

Florida Investor-Owned Utilities' Customer Data Security Information	FPL	FPUC	GR	PEF	TECO
Emphasis on data security (new employee training, ethics standards instruction / statements, coaching, and supervision)		Yes			
Proactive data security programs (IT, Customer Service, Payment Processing)		Yes			
Audit of IT / Customer Data in the last 24 months		No (begins 09/07)			
Number of security breaches, last 24 months		0			
Number of IT auditors		0			
Employs IT "defense in depth" using a combination of Intrusion Detection, Intrusion Prevention, virtual and physical measures to counter risks		No			
Masking of customer social security numbers (SSN)		Last 4 digits visible			
Total number of employees		352			
Number of employees with access to customers' full social security number		15			
Percentage of employees with access to customers' full social security number		4.3			
Number of employees with access to customers' banking account information		15			
Percentage of employees with access to customers' banking account information		4.3			
Number of employees with access to customers' date of birth information		n/a			
Work-at-home program for Customer Service Representatives		No			
Share customer information with an authorized third party over the telephone		Yes			

Source: Company Responses to Staff Document Requests 1 and 2

APPENDIX C

TREATMENT OF SENSITIVE CUSTOMER DATA

Florida investor-owned utilities collect, use, and mask a variety of sensitive customer information. Collection, use, and masking of information in each company is controlled and safeguarded by a combination of written policies, employee procedures, and management supervision practices. Virtual and physical security measures in each company round out the system designed to protect the data. The following chart summarizes the information each company collects, uses, and masks.

	Collects	Uses	Masks
[illegible]			
Social Security Number			
Driver's License Number			
Bank Account			
Date of Birth			
Credit Card Info			
[illegible]			
Social Security Number	X	X	X
Driver's License Number	X	X	X
Bank Account	X	X	X
Date of Birth			
Credit Card Info			
[illegible]			
Social Security Number			
Driver's License Number			
Bank Account			
Date of Birth			
Credit Card Info			
[illegible]			
Social Security Number			
Driver's License Number			
Bank Account			
Date of Birth			
Credit Card Info			
[illegible]			
Social Security Number			
Driver's License Number			
Bank Account			
Date of Birth			
Credit Card Info			

Alteration of employee status (e.g. retirement, position change, termination) is manually entered into the system. The HR Director has the responsibility. Policy is "a week or two". An email is sent to IT. IT removes or alters access as appropriate. Upon termination, all employees have a checklist to complete, with network access rights discontinued immediately upon termination notice.

Julie Petty, Director of Customer Relations, also has audit responsibilities. There have been no data security audits in the last 24 months. Crowe Chezik has been contracted to begin such an audit in September. The audit is scheduled for completion 10/07. All auditing is outsourced; FPU has no staff auditors.

(4) Data Request(s) Generated:

(5) Follow-up Required:

4.0 Florida Public Utilities

The two electric divisions of Florida Public Utilities Company (FPU) have 76 full-time and no part-time employees that services the electric divisions, and serves approximately 28,000 electric customers in Florida. The Northwest Division, headquartered in Marianna, provides service to customers in the western panhandle. The Northeast Division serves Amelia Island and is located in Fernandina Beach.

Deleted: 346
Deleted: 6
Deleted: .

4.1 Management Oversight

Does Florida Public Utilities management have a clear understanding that information security is a management responsibility?

FPU management acknowledges that information security is a management responsibility. According to FPU, company management sets the corporate climate for information security by creating procedures and determining information security priorities.

FPU management states that it recognizes that information security is only possible, and produces the best results, in a cooperative partnership with company employees. Further, the company states its objective relevant to information security is to create and sustain a workforce aware of the obligation to effectively manage and protect sensitive customer information. FPU managers stated that the company seeks to accomplish this objective through a comprehensive employee training program, management supervision of the workplace, employee mentoring, retraining (when necessary), and annually requiring all employees to acknowledge and sign the "Security of Customer Data" policy statement.

According to the company, managers and supervisors also routinely monitor software applications, programs, workstations and employee access to sensitive information to determine inherent operational risk. Changes in employment status, or an employee's business need to access sensitive customer data, are reported by managers to IT. Then, the employee's network access rights are revised to reflect the change, minimizing risk.

What type of personal information does Florida Public Utilities collect from customers?

The Customer Information System (CIS), a customer service and billing system, is used to initiate new accounts, update record information, and to store individual customer data. When initiating a new residential account, customer service representatives (CSRs) collect personal information from the account holder including the full name, social security account number, driver's license number, address, and phone number.

FPU service representatives also collect banking information if the customer wishes to establish automatic electronic payments. During initiation, customers also have the opportunity to provide names of others authorized to discuss the account, such as a spouse or other relative.

Has Florida Public Utilities management assessed the appropriateness of the information collected from customers?

FPU routinely collects both a social security number and driver's license number from a majority of its customers. According to the company, a social security number is required in order to run a credit worthiness check. Thereafter, the social security number is maintained for identification purposes and possible future collection actions.

The company reported that new customers are increasingly wary of identity theft and often do not wish to provide a social security number. In such cases, the driver's license number can be used as an alternative method of identification and to assist in possible future collections action. The driver's license information is maintained for the life of the account, all but the last four digits are masked, and FPU management does not perceive any undue risk in collecting or keeping this information.

Staff believes that requiring a driver's license number for identification purposes in the absence of a social security number may be appropriate. But, in the event that a social security number is obtained for identification and credit check, the additional need for collecting and maintaining driver's license information is not apparent. Staff believes that collecting any personal information beyond that which is absolutely needed poses unnecessary risk.

Does Florida Public Utilities adequately limit the use and disclosure of customers' personal information?

FPU has operational practices for customer service personnel to follow that address the use, disclosure, and retention of sensitive customer data. FPU has 10 customer service representatives in their electric divisions, 2 customer service supervisors, and 2 customer service managers to initiate new accounts and respond to other customer inquiries. Corporate headquarters is in West Palm Beach, but all payment processing is done in the Marianna office. The Director of Customer Relations supervises the billing of customers in both divisions.

Confidential

[redacted]

Service Manager and General Manager of the Northeast division, the Customer Service Manager and General Manager of the Northwest division, the Director of Customer Relations, and the Customer Information Manager. Customer Service Managers or General Managers make an information request to either the Director of Customer Relations or Customer Information Manager who is able to request IT to query the database for the requested information. [redacted]

Deleted: 32
Deleted: 4
Deleted: 5
Formatted: Highlight
Formatted: Tabs: 0.84", Left
Deleted: [redacted]
Deleted: [redacted]
Deleted: [redacted]
Deleted: [redacted]
Deleted:
Deleted: [redacted]
Formatted: Highlight

"[redacted]

Confidential

FPU procedures prohibit discussing confidential customer information with anyone other than the account holder, unless the requestor was previously authorized by the account holder. This restriction also applies to walk-up or telephone inquiries. When a non-account holder inquires, the CSR asks the individual for his or her name. For walk-ins, CSRs confirm pre-existing authorization and then view personal identification, such as a joint checking account or driver's license, prior to discussing an account. On the phone, CSRs ask for a name and then request additional confirmation. [redacted] Most account holders establish an authorized third party during account initiation. However, CSRs do not normally ask new customers whether they wish to establish another authorized user.

Formatted: Highlight

Formatted: Not Highlight

Formatted: Font color: Lime, Not Highlight

Formatted: Highlight

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

FPU managers stated that the company recognizes the inherent data security risk associated with any employees remotely accessing the network. Each Division General Manager and Operations Manager has remote access authorization to those portions of the network containing sensitive customer information. Nine IT employees also have the capability to access the network remotely. The company stated that it believes proper controls are in place to appropriately limit access.

What controls have Florida Public Utilities put in place for remote access of customer personal information?

Under normal operating conditions, remote access is limited to Division General Managers and Operations Managers. FPU does not allow customer service representatives to remotely access the network and has no work-from-home program. Management stated there is no current or anticipated need to undertake such a program. FPU has a post-hurricane contingency plan which would allow CSRs remote access if normal operations were rendered impossible due to extensive damage to company offices. [redacted] The virtual private network, or VPN, connects to a secure concentrator at the corporate office.

Formatted: Highlight

4.2 Information Technology Controls

Has Florida Public Utilities established an appropriate data security management function?

FPU's Director of Information Technology directly reports to the President & CEO. The IT Director has nine employees working in the information technology division.

According to FPU management, information management and security are the responsibility of all FPU personnel. FPU's Information Management (IM) section is specifically designated with the responsibility to assess the risks and potential vulnerabilities to the overall network and individual workstations. IM managers coordinate with, and provide technical advice to, company operational management in order to determine FPU policy, practices, and procedures relative to the handling, retention, and protection of sensitive customer data.

IM personnel also have the responsibility to monitor employee access to the network, its functions, and stored information. System usage is monitored, and the IM section processes all changes to employee network access. A change in employment status, such as retirement, termination, promotion, or transfer prompts an immediate review of access and any appropriate changes to authorization.

Has Florida Public Utilities established appropriate information security policies, procedures, and guidelines?

FPU information technology employees seek to establish appropriate information security policies, procedures, and guidelines in a variety of ways. These include:

Confidential

[redacted]

Confidential

Information Management employees also 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 to enhance programs.

[redacted] Only software patches produced by authorized vendors are used [redacted] As a further precaution, no patch is installed until it has been first tested to ensure its compatibility with current network configurations and will not harm existing programs or data.

Operational managers coordinate with information management throughout each phase of the patch process. They receive testing results, evaluate the effects, and assess risk for each patch prior to full uploading on the existing network. Only company management can authorize a system-wide installation of patches based on test evaluation and risk assessments.

FPU information management is planning two significant improvements directly linked to information security. The first is an upgrade to existing Cisco wireless access devices to the next level of available security. Second, the company will be raising security certificates to the 128-bit encryption level.

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

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

CONFIDENTIAL

Formatted: Font: 12 pt

According to FPU management, information security is not possible without parallel security of the Information Management (IM) parent site located in West Palm Beach. Access to this facility is controlled by a magnetic lock. [redacted]

Formatted: Highlight

Confidential

[redacted]

Formatted: Highlight

Does Florida Public Utilities restrict access to customer information related software functions, data, and programs?

The company network has many levels of resident security. All users must have a valid user name and password. Access is authorized based on a business need-to-know and contingent on approval by both supervisors and information management. Access to different parts of the network is derived from a menu at each workstation, tailored to individual users. Lack of the appropriate level of access authority will result in denied access. Different programmers have either very wide or universal network access, but are subject to continual monitoring.

Confidential

[redacted] The *Global Technology Audit Guide (GTAG)* establishes best practices for information security, derived from industry sources worldwide. These practices support effective information security management and, when used, significantly reduce the risk of compromise. A key component of these practices is employing a defense in depth, a system of active and passive measures to thwart network compromise. The premise of defense in depth is to layer physical and virtual security, combining passive intrusion detection systems and active intrusion prevention systems. [redacted]

Formatted: Highlight

Deleted: [redacted]

Formatted: Font color: Auto, Highlight

Deleted: [redacted]

Formatted: Highlight

Formatted: Highlight

Does Florida Public Utilities monitor software security activity and produce appropriate management reports?

FPU information management has the ability to monitor employee access to the network and sensitive information in real time. This oversight provides IM 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.

The information management system automatically monitors and captures software and access activity around the clock. The results are available for regular review by IM personnel. Network information is then routinely made available to management in the form of two reports, the *Access Report* and the *Use Report*. These are also available on very short notice through a request to IM. The *Access Report* pinpoints who within FPU has current access authority for all network functionalities, while the *Use Report* documents employee usage on the network, sites visited, and e-mails.

4.3 User Awareness and Training

Does Florida Public Utilities have adequate privacy and data security policies and procedures?

Annually, FPU policy requires all employees to read and acknowledge by signature the *Florida Public Utilities Code of Ethics*, dated February 2005 and the *Employee Conduct and Work Rules.* However, the *Florida Public Utilities Code of Ethics* only briefly addresses the handling of sensitive customer information and does not site specific laws or regulations. Due to the relatively small size of FPU, all signed copies for 2007 from Marianna Division employees were verified. The *Employee Conduct and Work Rules* policy defines unauthorized disclosure of confidential information as sufficient for disciplinary action. The *Computer, E-mail, Voice Mail, and Internet Use* policy outlines proper use of these functionalities, but does not address customer sensitive data specifically.

Though these policies do not specifically focus on the protection of sensitive customer information, FPU management states that it believes each policy helps create an employee mindset that is conducive to safeguarding customer sensitive data, and transferable to the application of such safeguards.

Security of Customer Data is a specific data security policy and procedure requiring full understanding and acceptance by all employees. New employees must read and acknowledge the policy by signature upon completion of initial training and annually thereafter.

Are Florida Public Utilities employees properly trained on privacy and data security policies?

According to the company, an expectation of ethical behavior regarding the handling of sensitive customer information is incorporated into the FPU training program. FPU provides formal initial training for all new employees using a combination of written policies, established practices, and standardized procedures pertaining to the security of sensitive customer information. As a part of this training, each employee is required to read and sign the *Security of Customer Data* policy and procedure notice.

Trainers from the West Palm Beach headquarters visit the divisions up to four times annually, conducting refresher training for all employees. According to FPU, there are always customer service and data security components to this training. On-the-job training is used to augment the initial training of new customer service representatives. A new customer service representative first shadows a more senior

employee and, later, the roles are reversed. When the new employee demonstrates a thorough knowledge of correct customer procedures and data safeguards, he or she is allowed to work without direct, constant supervision. Every supervisor and manager attended supervisory training in May of 2007. The training was conducted by the corporate attorney and included instruction on company policies pertaining to privacy, data security, and ethics.

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

Florida Public Utilities' *Progressive Disciplinary Procedure* policy establishes a formal five-step disciplinary process which escalates in severity from a first (verbal warning) to fifth step (termination). At the lower end of the severity scale, FPU commonly combines mentoring and retraining verbal or written warnings to redress conduct violations. Depending on the nature and severity of the misconduct, the process can be accelerated.

4.4 Outsourcing Controls

Does Florida Public Utilities provide third parties with access to customer personal and / or banking information?

Florida Public Utilities does not outsource customer services. The CIS billing vendor with which FPU has a service/support agreement has access to customer records in CIS in order to diagnose and correct billing-related errors. The only other outside vendor with access to customer information is the company auditors.

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

FPU uses confidentiality clauses whenever contracting for third party audit or repair service and support. These clauses require the third party to adhere to FPU protocols, policies, and procedures regarding sensitive customer information. Company management believes the current confidentiality agreements, in contracts between FPU and outside firms, adequately safeguards customer information.

Confidential

[redacted]

Formatted: Highlight

Deleted: [redacted]

FPU states that it further limits the risk of personal information disclosure by choosing not to use satellite company payment locations or authorized third party payment stations.

4.5 Auditing Controls

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

FPU does not employ full time staff auditors. The auditing firm of Binder, Dijker, Otte & Company (BDO) is the external auditor for FPU. BDO, an international accounting firm, was founded in Europe in 1963. US offices were established in 1988. BDO's auditing expertise is in finance and accounting. BDO conducted a financial audit annually for FPU during the two year period covered by this review. Binder, Dijker, Otte & Company audits do not focus specifically on information technology or information security. However, FPU stated that the BDO audit findings still provide general insights on data security and network protection.

Crowe Chezik is the FPU internal auditor. Founded in 1942, Crowe Chezik is one of the top ten public accounting and auditing firms in the nation.

Does Florida Public Utilities periodically assess the organization's information security practices?

No audit of FPU information security practices was performed over the period 2005 to September, 2007. However, FPU has recently initiated an audit of network security and risk assessment by Crowe Chezik, their internal auditors. The audit will focus on Sarbanes-Oxley IT controls. Completion of the audit is anticipated in October 2007.

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 Florida Public Utilities' corporate and IT management?

Florida Public Utilities has no internal audit department. Matters relating to information management are the responsibility of management and IT personnel. In the event of any breach or compromise to sensitive customer data, the incident and pertinent facts surrounding it are required by company policy to be reported to both.

Management stated that there have been no detected incidents of internal or external sensitive information compromise during the last two years. According to the company, there has not been a single theft or loss of data, disks or other storage media, laptops, or an external compromise of any sort to the network.

4.6 Conclusions

Confidential

With significantly fewer customers, employees, and other assets at its disposal, FPU's depth and breadth of measures to safeguard sensitive customer information

Formatted: Font: 12 pt

Formatted: Highlight

[redacted]

Formatted: Highlight

Confidential

[redacted]

Formatted: Highlight

[redacted]

CONFIDENTIAL

STATE OF FLORIDA

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

Public Service Commission

ACKNOWLEDGEMENT

DATE: December 17, 2007

TO: Norman Horton/Messer Law Firm

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 080063-EI ~~070000~~ **or, if filed in an undocketed matter, concerning** portions of staff report entitled, "Customer Data Security of Florida's Five Investor-Owned Utilities", **and filed on behalf of** Florida Public Utilities. **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.