

Memorandum

TO: Honorable Mayor and City Council Members

FROM: Linda Snyder, Financial Services Supervisor



DATE: October 22, 2008

SUBJECT: Identity Theft Detection Resolution 509-08

PURPOSE

Adherence to Fair and Accurate Credit Transactions (FACT) Act of 2003, Identity Theft Red Flag Ruling by the adoption of Identity Theft Detection and Prevention Program.

BACKGROUND

The Federal Trade Commission (FTC) recently adopted rules on identity theft “red flags” (i.e., warning signs) pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. The new rules, which require action by November 1, 2008, require any business with a “covered account” to adopt and implement an identity theft program. The City of Orange City and other cities that operate a municipal utility will be affected by these new rules.

A covered account is one where an entity (such as a municipal utility) provides a service or good before the consumer pays for it. For example, most municipal water utilities provide water to the customer, and then bill the customer later based on consumption.

A city with such accounts must, by November 1, 2008, adopt and implement a written program that: (1) identifies relevant identity theft “red flags” to the utility or other covered entity; (2) provides for detection of those red flags; (3) provides for appropriate responses to any red flags that are detected; and (4) ensures that the program is updated periodically to address changing risks.

The adoption of the attached policy “Exhibit A” is the first step to bringing Orange City into compliance. After Councils acceptance of the program, Customer Service Specialists shall receive training and the Privacy Committee shall conduct an organizational meeting. To remain in compliance the committee shall continue to meet and report any incidents of Identity Theft to the City Manager on an annual basis, or as need arises.

RECOMMENDATION

Staff recommends that the City Council approve Resolution No. 509-08.

RESOLUTION NO. 509-08

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF ORANGE CITY, FLORIDA, ADOPTION OF IDENTITY THEFT DETECTION AND PREVENTION PROGRAM; REPEALING ALL RESOLUTIONS IN CONFLICT HEREWITH AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, The Fair and Accurate Credit Transactions Act of 2003 (FACTAct) was signed into law amending the Fair Credit Reporting Act (FRCA) in an attempt to help prevent identity theft. Compliance with the Act is required by November 1, 2008; and

WHEREAS, Section 114 of the FACTAct requires “each financial institution or creditor to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft”; and

WHEREAS, The City of Orange City, more specifically Orange City Utilities is considered a creditor, as a municipal utility where a service or good is provided before the consumer pays for it; and

WHEREAS, a city with such accounts must adopt and implement a written program that: (1) identifies relevant identity theft “red flags” to the utility or other covered entity; (2) provides for detection of those red flags; (3) provides for appropriate responses to any red flags that are detected; and (4) ensures that the program is updated periodically to address changing risks.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF ORANGE CITY, FLORIDA:

SECTION 1. The City Council of the City of Orange City adopts the Identity Theft Detection and Prevention Program, attached as “Exhibit A”.

SECTION 2. The City of Orange City and Orange City Utilities shall be in compliance with The Fair and Accurate Credit Transactions Act of 2003 (FACTAct).

SECTION 3. That all resolutions or parts of resolutions in conflict herewith be and the same are hereby repealed.

SECTION 4. This Resolution shall become effective immediately upon its adoption.

ROLL CALL VOTE AS FOLLOWS:

Jim Mahoney	_____	Donald C. Sherrill	_____
Donald Sandford	_____	Tom Abraham	_____
Tom Laputka	_____	Jeff H. Allebach, Vice Mayor	_____
Harley Strickland, Mayor	_____		

ADOPTED THIS _____ DAY OF _____, 2008.

ATTEST:

AUTHENTICATED:

Deborah J. Renner, CMC, City Clerk

Harley Strickland, Mayor

Approved as to form and legal sufficiency:

William E. Reischmann, Jr., City Attorney



Orange City Utilities

Identity Theft Detection and Prevention Program

In Compliance with the Federal FACT Act (2003)

Identity Theft Red Flag Ruling

October 21, 2008

Provided by: Florida Municipal Electric Association (FMEA)

Purpose

The goal of this policy is to prevent identity theft pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. Orange City Utilities recognizes the responsibility to safeguard customer's personal information during its collection, recording and handling with all Orange City Utilities branches and workplace. The purpose of this policy is to create an Identity Theft Detection and Prevention Program utilizing guides set forth in the FACTAct (2003).

Scope

This policy applies to management and all personnel of Orange City Utilities. The following represents a policy for the development of the identity theft detection and prevention program. Any part or the whole of policies and procedures written and developed will be incorporated into the program where appropriate. This does not replace, but rather supplements, any of Orange City Utilities standing policies.

Responsibility

Orange City Utilities must protect its customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by November 1, 2008. Thereafter, Orange City Utilities will continually report and monitor the program's integrity, completeness, and deficiencies. Any oversight or patches to perfect the program will be reviewed and amended annually.

Definitions

Identity Theft- Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim or Orange City Utilities. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit cards accounts, establishing line of credit, or gaining access to the victim's accounts with the intent of depleting the balances or avoid payments to services delivered by Orange City Utilities.

Red Flag-A pattern, particular specific activity that indicates the possible risk of identity theft.

Privacy Committee

Orange City Utilities' Privacy Committee is established to create, drive, and monitor the program. A Privacy Officer functions as the head of the committee and reports to a member of Senior Management regarding the outcomes and needs of The Identity Theft Detection and Prevention Program. The following positions shall provide input to enhance the program, attendance is optional, additional departments or resources may be called upon as deemed necessary.

Department	Role
Privacy Officer	Coordinates audit studies and reviews pattern of incidents.
Senior Management	Supplying resources to establish proactive identity theft program.
Accounting	Billing Collections Expert in the flow of funds.
IT	Data and Network Security-Expert in SCADA/network administration.
Human Resources	Personnel Information. Identity Theft Training.
Customer Service	Day to day processes in opening new accounts and monitoring activity on existing accounts.
General Counsel	Provide insights in legal ruling and State Statutory clarifications.
Police Department	Provide insights in prevention and trends.

Policies & Procedures

A. Red Flags Identification and Mitigation Polices

Flag	Next Step	Mitigation
Alerts		
Presentation of Suspicious Documents		
Identification documents appear altered or forged	Ask the customer to visit the issuing agency (DMV) and get an acceptable copy of the suspicious document	Do not open the account
Photo/physical description does not match applicant.	Ask the customer to visit the issuing agency (DMV) and get an updated copy of the identification document	Do not open the account
Other information on identification is inconsistent with information given on the application. Example-last name is different.	Ask the customer to verify the inconsistent information with supporting documentation such as marriage certificate or social security card	If customer is able to verify information, no further action should be necessary

Information in utility files is inconsistent with information provided. Example- signatures do not match on signature card.	Inform the customer of the discrepancy and ask the customer to verify the inconsistent information with supporting documentation such as signature on driver's license	It may be appropriate to notify law enforcement if a customer who is able to verify his identity to you believes his signature card has previously been forged in connection with identity theft
Application looks altered or forged or destroyed and reassembled.	Ask the customer to fill out another application in the office and verify all suspicious information	Do not open the account unless you are able to verify the information on the application

Flag	Next Step	Mitigation
Alert		
Suspicious Personal Identifying Information		
Identification is inconsistent with external information source.	Ask the customer to verify the information with supporting documentation such as social security card and driver's license	If customer is able to verify information, no further action should be necessary
Applicant fails to provide all personal ID requested.	Inform the customer of the requirements to open an account and direct them where they can obtain this documentation if they do not already have it.	Do not open the account unless you are able to verify the identity with other types of acceptable documentation or have customer provide the deposit associated with not having proper identification.
Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account).	Verify the identity of all persons requesting address changes, adding properties, or changing authorized users.	If you are able to verify the identity of the person making the request, then no further action should be necessary
Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	Contact the customer	Close inactive accounts after a reasonable period of time

Mail sent to customer is repeatedly returned.	Contact the customer to verify the correct billing address	If you are able to verify the correct address and then change the address on file, no further action should be necessary
---	--	--

Flag	Next Step	Mitigation
Alert		
Customer notifies utility that they are not receiving their bill.	Verify the identity of the customer and then verify the correct address	If you are able to verify the correct address and then change the address on file, no further action should be necessary
The utility is notified of unauthorized charges or transactions in connection with a customer's account.	Ask the customer to supply documentation regarding the possible of identity theft such as an Affidavit or police report	Notify law enforcement
Notice of Identity Theft		
Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.	Follow the instructions of law officials	Depending on what law enforcement asks you to do, you may close or closely monitor the account

B. Handling a Breach in Security

To prevent identity theft by Orange City Utilities employees, limit exposure of secured information by creating a professional standard. Implement a "need to know" policy with all confidential information. Train management to recognize signs of employee theft including sifting through waste receptacles, downloading excessive amounts of consumer information, using secured terminals without authorization, etc.

C. Handling an Address Discrepancy

Report address discrepancies in accordance with consumer report, when utilizing such services.

D. Record Disposal

Utilities need a written program outlining how to maintain and shred documents and destroy data:

- ✓ Well-defined step by step procedures for handling various types of data and documents.

- ✓ Procedures for collecting and protecting documents and data until the time of destruction.
- ✓ Documentation of Record Destruction.

Best Practices:

- ✓ Placing shredders next to trash cans and copiers enhance employee compliance.
- ✓ Train Customer Service Representatives and any other employees who at times make hand written notes to destroy after data is entered.

E. Training and Screening

- ✓ Run background check, thorough screening, and ask specific scenario questions at hiring.
- ✓ Train employees to identify Red Flags.
- ✓ Following the “need to know” rule, employees, will receive only the information that relates to their specific job.
- ✓ Supervisory training will involve additional information including managerial responsibilities in identity theft prevention.

F. Handling Reports of Suspected Identity Theft

When the consumer suspects Identity Theft, they must notify the OCU in writing, filling out the appropriate form. Make copy of consumer’s photo ID and attach it to the police report along with the completed form and send all to the privacy officer.

- ✓ Close or block breached account and open new account.
- ✓ Place an alert to notify Customer Service of the situation.
- ✓ IT IS CRITICAL THAT NO INFORMATION BE GIVEN DIRECTLY TO THE CONSUMER UNTIL THE INVESTIGATION IS COMPLETE. The privacy officer will determine the course of action at this point.

G. Victim Record Request

Under the FACTAct, identity theft victims are entitled to a copy of the application or other business transaction records relating to their identity theft free of charge. Utilities must provide

these records within 30 days or sooner of receipt of the victim's request. Businesses must also provide these records to any law enforcement agency which the victim authorizes.

Before providing the records to the victim, the utility must ask victims for:

- a. Proof of identity, which may be a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information currently requesting from applicants or customers and
- b. A police report and a completed affidavit.

H. IT Security

The network administrator and IT management will review audit logs that are generated by point of entry systems to the network on a regular basis. Point of entry systems include but are not limited to, e-mail, application, and web-mail servers. These logs are currently already checked on a daily, weekly, and monthly basis, as a result of suspicious or extraordinary network activity producing an alert during normal operations. All persons having console access to these systems will sign agreements to not disclose private information.

I. Medical Confidentiality

Orange City Utilities shall not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for services.

J. Reports, Reviews, and Updates for Policy Enforcement

Periodically, internal staff and auditors, external auditors and accountants, and government regulators will review practices to ensure compliance. The reports will be used to evaluate effectiveness of and amend the Identity Theft Prevention Program.

An annual report reviewing all incidents, program revisions and goals will be submitted to the City Manager each January, starting in 2010, with a copy provided to the City Auditor.

Reporting Tools

The following forms will be used to report Identity Theft Incidents:

**Identity Theft Prevention Program Incident Report
Orange City Utilities**

Date: _____

Prepared by: _____
(Employee Designated to track and record information)

Committee Members:

It is the policy of Orange City Utilities to provide an Identity Theft Prevention Program for customers and employees. The purpose of this report is to promote continued evaluation of effectiveness of current policies and procedures in compliance with the FACTAct (2003). This document will be used to drive recommendations for changes to the program due to evolving risk and methods of theft.

(Annual (January) to City Manager, copy to Auditor)

