City of Plant City

Identity Theft Detection and Prevention Program

In compliance with the Federal FACT Act (2003)

Identity Theft Red Flag Ruling

City of Plant City

Identity Theft Detection and Prevention Program

Table of Contents

Page

General Information

A ruling known as the 'Identity Theft Red Flags Regulation' was jointly issued by the Federal Trade Commission, Office of Thrift Supervision and several other governing agencies; implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT ACT) and is effective on November 1, 2008.

The Identity Theft Red Flags Regulation requires financial institutions to develop and implement a written Identity Theft Program to detect, prevent and diminish identity theft in connection with opening of certain accounts or certain existing accounts.

Under the regulation only those financial institutions that offer or maintain 'covered accounts' must develop and implement a written program. A 'covered account' is defined as *(1) an account primarily used for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.*

The *Agencies* believe that accounts such as credit cards, mortgage loans, cell phone, utility, checking, automobile loans, and savings accounts are examples of accounts designed to permit multiple payments or transactions and also contain a reasonably foreseeable risk of identity theft.

Purpose

The goal of this policy is to prevent identity theft. City of Plant City recognizes the responsibility to safeguard customer's personal information during its collection, recording and handling within all City of Plant City branches and workplace. The purpose of this policy is to create an Identity Theft Detection and Prevention Program utilizing guides set forth in the FACT Act (2003).

Scope

This policy applies to management and all personnel of City of Plant City. 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 City of Plant City's standing policies.

Responsibility

City of Plant City must protect its customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by November 1, 2008. Thereafter, City of Plant City will continually report and monitor the program's integrity, completeness, and deficiencies. The Privacy Committee will review the program annually and amend policy when necessary.

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 City of Plant City. This fraudulent activity may include opening utility accounts with counterfeit checks, using stolen identification for setting up new accounts or gaining access to the victim's accounts with the intent of using services under the name of someone else in order to avoid payments of services delivered by City of Plant City.

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

Identifying Information - Any name or number that may be used alone or with any other information to identify a specific person; includes name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport and employer or tax identification number.

Privacy Committee

City of Plant City's 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 or City Manager regarding the outcomes and needs of The Identity Theft Detection and Prevention Program.

Position	Name	Role
Utility Billing Manager	Denise McDaniel	Privacy Officer – Coordinates audit and reviews pattern of incidents. Expert in flow of funds.
Finance Director and Assistant Finance Director	Martin Wisgerhof Linda Hill	Senior Management – supply recourses to establish proactive Identity Theft Program.
Customer Service Clerk IV	Carlye Vickers	Expert in day to day processes in opening new accounts and monitoring activity on existing accounts.
Customer Service		Provides insight in collection policies and procedures

Policies & Procedures

A. Red Flags Identification and Mitigation Policies

Flag	Next Step	Mitigation
Alerts		
Credit Card declined	Tell the customer about the alert and ask the customer to contact the Credit Reporting Agency or Credit Card Company to resolve the issue	Do not open the account
Notice of address discrepancy	Ask the customer to verify the address with supporting documentation	If the customer is able to verify address, Open the account and make necessary changes to the billing system if necessary
Unusual patterns in activity – consumption on closed account, multiple returned checks, multiple credit card fraudulent claims filed using same customer's name	Contact customer for verification	Terminate services Accept other forms of payments
Presentation of Suspicious Documents		
Identification documents appear altered or forged.	Ask the customer to visit the (DMV) and get an acceptable form of identification	Do not open account
Photo/physical description does not match applicant.	Ask the customer to visit the (DMV) and get an acceptable form of identification	Do not open account
Other information on identification is inconsistent information given from applicant	Ask the customer to verify the inconsistent information with supporting documentation such as birth certificate, social security card	If customer is able to verify information, no further action should be necessary

Flag	Next Step	Mitigation
Presentation of Suspicious Documents		
Information in utility files is inconsistent with information provided. Example – signatures do not match on Senior Citizen discount form.	Inform the customer of the discrepancy and ask the customer to verify the inconsistent information with supporting documentation such as driver's license or come inside for signature verification	Inform law enforcement if the customer identified believes that the application was forged or it has been connected 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
Suspicious Personal Identifying Information		
Identification is inconsistent with external source such as: • Address vs. Address on Lease	Ask the customer to contact Landlord for verification of address	If the customer is able to verify address, Open the account
• Social security number not issued.	Tell the customer about the Social Security discrepancy and ask them to contact a Social Security representative to resolve the issue	Do not open the account
• Social security number on Death Master File.		
• Inconsistent information, such as lack of correlation between date of birth and social security number.	Ask the customer to verify information with supporting documentation such as social security card and driver's license	If the customer is able to verify information, no further action should be necessary

Flag	Next Step	Mitigation
Suspicious Personal Identifying Information		
Identification is known to be associated with fraudulent activity: • The Address is fictitious, a prison or a mail drop on application. • The phone number is invalid or associated with a pager or answering service. • The Social security number is the same as that submitted by other persons opening an account. • The Address is the same address as that submitted by other persons opening an account.	Check to be sure that the property is not associated with rental property	Do not open the account if it is not part of a rental group or landlord with multiple addresses If the identification address is a mail drop or prison address, get another form of identification that is current, possible Parole Release Letter listing current address It may be appropriate to notify law enforcement if a customer who is able to verify his Social Security Number believes his number has been used in connection with identity theft.
Applicant fails to provide all personal ID requested.	Inform the customer of the requirements to open an account and direct them to where they can obtain this information – DMV for driver's license and Landlord for lease or Ownership papers	Do not open the account until you are able to verify the identification with other types of acceptable documentation
The person attempting to access cannot provide password.	Ask the customer to provide Driver's License number for verification purposes	If customer is able to verify DL, allow access to the account, if not Do not give access
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
Lease submitted for proof of residency appears to be altered or forged	Ask the customer to supply an unaltered lease with the Landlord's signature notarized.	Do not open the account unless you are able to verify the residency requirement.

Flag	Next Step	Mitigation
Suspicious Personal Identifying Information		
Mail sent to customer is repeatedly returned by Post Office.	Contact the customer to verify the correct billing address	If you are able to verify the correct address, change the address on file and no further action is necessary
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, change the address on file and no further action is necessary
The utility is notified of unauthorized access 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 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	You may be asked to terminate or closely monitor the account

B. Handling a Breach in Security

To prevent identity theft by City 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

Occasionally, a person or agency requests a consumer report on one of our customers. If this report includes an address that substantially differs from the addresses in the consumer's file, and a response to the request is issued, the City should notify the person making the request of this discrepancy.

D. Disclosure of Personal Information

1) Information is used as a means of identification, for internal verification, administrative purposes, and for debt collection purposes.

2) The City of Plant City falls under the Public Records Law and all records are open to inspection. Chapter 119, Florida Statutes, commonly known as Florida's "Public Records Law," provides information on public records in Florida, including policies, definitions, exemptions, general information on records access, inspection, examination and duplication of records. Florida's public records laws are very broad, and most documents and records are available to the public. However, the laws do provide specified exceptions such as social security numbers.

E. Data Retention and Disposal

Records are disposed of in accordance with state and federal law, including the local records retention schedule issued by the State of Florida General Records Schedule for State and Local Government Agencies and Public Utilities. Documents with sensitive information are disposed by shredding.

F. Training and Screening

A copy of the Identity Theft Detection and Prevention Program will be given to all Customer Service Employees. Initial training sessions will be set up to help the employee identify "red flags" and explain the policies and procedures. The Identity Theft Program will be included in the initial training of all new employees.

All employees undergo a background check conducted by the Human Resources Department prior to hiring. Employees are assigned security levels which limit access to sensitive data. The System Administrator provides the initial password for each employee to access the system.

All employees with access to the American Data Group utility program shall sign an agreement to not disclose private information.

G. Handling Reports of Suspected Identity Theft

When the consumer suspects Identity Theft, they must notify the City 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 account.
- ✓ Place an alert on location master and 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.

H. Victim Record Request

Under the FACT Act, 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 the business is currently requesting from applicants or customers and

b. A police report and a completed affidavit, which may be either the FTC Identity Theft Affidavit (included) or the business's own affidavit.

I. IT Security

The network administrator and IT management may conduct audits on a quarterly basis.

J. Reports, Reviews and Updates for Policy Enforcement

Periodically, internal staff and auditors who report to the City Manager, external auditors and accountants, and government regulators will review practices to ensure compliance with corporate policy. 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 year.

Reporting Tools

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

Identity Theft Prevention Program Incident Report (City of Plant City)

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

Committee Members:

_____

_____

_____

_____

_____

_____

_____

It is the policy of City of Plant City 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 FACT Act (2003). This document will be used to drive recommendations for changes to the program due to evolving risk and methods of theft.

Identity Theft Prevention Program Incident Report

Page 2

Date	Scope	Employee	Employee Trained	Incident/"Significant Event"	Management Response	Mitigation

Identity Theft Prevention Program Incident Report
Page 3

Describe current strengths of Utility Identity Theft Program:

Describe areas for Improvement:

Goal for Improvement	Steps Needed	Person(s) Responsible	Date

Committee Signatures

(Name)	(Title)	(Date)
(Name)	(Title)	(Date)
(Name)	(Title)	(Date)
(Name)	(Title)	(Date)