RESOLUTION NO. 2009- 131

A RESOLUTION OF THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, ADOPTING THE ST. JOHNS COUNTY UTILITIES DEPARTMENT IDENTITY THEFT PREVENTION PROGRAM, AND DESIGNATING THE COUNTY UTILITIES DEPARTMENT RED FLAG RULES COMPLIANCE OFFICER AS THE INDIVIDUAL CHARGED WITH ON-GOING OVERSIGHT OF THE COUNTY UTILITY DEPARTMENT IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, St. Johns County, Florida (the "County") finds that identity theft is a serious problem in the United States; and

WHEREAS, in response to the risks posed by identity theft to consumers and to the financial soundness of businesses, the United States Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACT Act); and

WHEREAS, the Federal Trade Commission (FTC), along with federal bank regulators, adopted regulations implementing the FACT Act (the Red Flag Rules) that require creditors to adopt a written Identity Theft Prevention Program; and

WHEREAS, St. Johns County Utilities Department believes it is a creditor subject to the FTC's Red Flag Rules; and

WHEREAS, St. Johns County Utilities Department has developed a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft; and

WHEREAS, a copy of the St. Johns County Utilities Department Identity Theft Prevention Program is attached and incorporated as a part of this Resolution; and

WHEREAS, the County has determined that approval of the St. Johns County Utilities Department Identity Theft Prevention Program is in the best interests of the County.

NOW THEREFORE, BE IT RESOLVED, by the Board of County Commissioners of St. Johns County, Florida, that:

Section 1. The above Recitals are incorporated by reference and made a part hereof as Findings of Fact.

Section 2. To the extent that there are typographical or administrative errors that do not change the tone, tenor, or concept of this Resolution, then this

Resolution may be revised without subsequent approval of the Board of County Commissioners.

Section 3. The St. Johns County Board of County Commissioners hereby approves the Identity Theft Prevention Program as submitted by St. Johns County Utilities Department.

Section 4. The St. Johns County Utilities Department Customer Service Manager, assigned as the Red Flag Rules Compliance Officer, has the delegated responsibility for oversight, ongoing development, implementation, and administration of the program and shall have the responsibility to develop periodic updates to the program to reflect changes in risk to customers and to the safety and soundness of the organization.

PASSED AND ADOPTED by the Board of County Commissioners of St. Johns County, State of Florida, this 5th day of May, 2009.

BOARD OF COUNTY COMMISSIONERS
OF ST. JOHNS COUNTY, FLORIDA

By: Cyndi Stevenson
Cyndi Stevenson, Chair

ATTEST: CHERYL STRICKLAND, CLERK

By: Pam Hatterman
Deputy Clerk

RENDITION DATE 5/7/09

St. Johns County Utilities Department
Identity Theft Detection and Prevention Program

May 2009

In Compliance with Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), also known as the RED FLAG RULES
Passed on October 31, 2007

Table of Contents

Purpose

St. Johns County Utilities Department (SJCUD) is committed to providing all aspects of our service and conducting our business operations in compliance with all applicable laws and regulations. This policy sets forth our commitment to compliance with those standards established by the Federal Trade Commission under the Identity Theft Red Flags under the Fair and Accurate Credit Transaction Act of 2003 ("the Red Flag Rules"), regarding the establishment of a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

Scope

This Program contains policies and procedures designed to identify, detect and respond appropriately to "Red Flags" for identity theft. It also contains policies and procedures for the periodic identification of covered accounts and for the general administration of the Program. This Program addresses our general approach to compliance with the Red Flag Rules. As a "creditor" with "covered accounts" under the Red Flag Rules, St. Johns County Utilities is required to:

- Periodically identify covered accounts;
- Establish a written Identity Theft Prevention Program; and
- Administer the Identity Theft Prevention Program.

Definitions

ACCOUNT means a continuing relationship established by a person with St. Johns County Utilities to obtain a product or service for personal, family, household or business purposes and includes an extension of credit, such as the purchase of property or services involving a deferred payment.

COVERED ACCOUNT means:

(i) An account that St. Johns County Utilities offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

CUSTOMER means a person that has a covered account with a financial institution or creditor.

IDENTITY THEFT means a fraud committed or attempted using the identifying information of another person without authority.

IDENTIFYING INFORMATION means a name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

RED FLAG means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

SERVICE PROVIDER means a person that provides a service directly to St. Johns County Utilities.

Part I. Assessment of Existing Business Practices

Part I of the Identity Theft Prevention Program is used to identify areas of potential risk within SJCUD standard Customer Service business practices. SJCUD has selected specific business processes associated with offering or maintaining accounts, or engaging in other activities that could raise "red flags" indicating the potential for identity theft.

A. SJCUD provides Customer Service personnel with the ability to request and review a customer's personal identifying information when engaging in any of the following activities:

- Open new accounts;
- Access existing accounts;
- Modify existing accounts; and/or
- Close existing accounts.

B. SJCUD provides customers with the ability to do one or more of the following actions independent of Customer Service personnel (either through an automated phone system or online), and a customer's personal identifying information is required to complete any of these activities:

- Open a new account;
- Access an existing account;
- Modify an existing account; and/or
- Close an existing account.

Also, if SJCUD has identified a past occurrence of identity theft that was linked to a customer's utility account (an unauthorized opening, modifying or closing of an account), then SJCUD must perform the actions set forth in the following Program.

Part II. Identification of Red Flags

Part II of the Identity Theft Prevention Program assists SJCUD in identifying Red Flags that may arise during routine handling of new and/or existing accounts. SJCUD has identified the following items as potential Red Flag sources or categories that might indicate an instance of identity theft.

- Consumer report includes a fraud or active duty alert, a notice of credit freeze and/or a notice of address discrepancy.

- Documents provided for identification appear to have been altered or forged.

- Photograph, physical description and/or other information on the identification is not consistent with the appearance of the person presenting the identification.

- Information on the identification is not consistent with readily accessible information that is on file with the Utility.

- Information provided is inconsistent when compared against external information sources (address does not match any address in the consumer report and/or social security number has not been issued or is associated with a deceased person).

- Information provided by the customer is inconsistent with other information provided by the customer (no correlation between SSN range and date of birth).

- Information provided is associated with known fraudulent activity (address and/or phone number on an application is the same as the address provided on a previous fraudulent application).

- Information provided is of a type commonly associated with fraudulent activity (address on an application is fictitious and/or phone number is invalid).

- Social security number, address and/or telephone number provided is the same as or similar to ones provided by another customer.

- Customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

- Customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

- Utility is notified that the customer is not receiving paper account statements.

- Utility is notified that it has opened a fraudulent account for a person engaged in identity theft.

Part III. Detection of Red Flags

Part III of the Identity Theft Prevention Program addresses the process of detecting Red Flags as related to possible identity theft during SJCUD's routine handling of new and/or existing accounts. The following is a list of detection methods that SJCUD uses to prevent identity theft.

- Require customers to present government-issued identification information to open a new account. Types of necessary information include:

    - Name
    - Date of birth

- Social security number
- Address
- Phone number
- Photo identification

- Verify personal identification information using records on file with SJCUD or through a third-party source such as a consumer reporting agency.

- Independently contact the customer (in the case of phone or internet setup of new utility accounts).

- When fielding a request to access and/or modify an existing account (such as a change of billing address), verify identity of customer by requesting specific pieces of personal identifying information (identification with the new billing address and/or documentation proving shift of financial liability)

- If new banking information is provided for electronic payment of accounts, cross-check ownership of the new banking account with the customer name on the utility account by contacting the appropriate financial institution.

- For online or automated phone system access of utility account, require the establishment of security questions during the initial set-up of the account.

Part IV. Prevention and Mitigation

Part IV of the Identity Theft Prevention Program details response actions for SJCUD personnel if the personnel have observed a Red Flag associated with a new or existing utility account. One of more of the following actions will be taken by SJCUD to rectify the situation.

- SJCUD will not open a new account (after review of the presented identifying information and discussion with department supervisor).

- For an existing account, SJCUD may discontinue the services associated with that account and/or:

    - Continue to monitor the account for evidence of identity theft and contact the customer to discuss possible actions.
    - Change the passwords, security codes, or other security devices that permit access to an existing account.
    - Reopen an existing account with a new account number.
    - Close an existing account.

- If SJCUD has identified an instance of identity theft associated with an unpaid account, SJCUD will not attempt to collect on the account or sell the account to a debt collector.

- If applicable, SJCUD will provide the consumer reporting agencies with a description of the identity theft event.
- For all instances of suspected or confirmed identity theft, SJCUD will notify local law enforcement and will provide them with all the relevant details associated with the identity theft event.

Part V. Program Administration

Program administration is an important part of the Identity Theft Prevention Program. This section details the training requirements, annual program review, approval and adoption process and annual reporting requirements that are associated with this Program.

A. Staff Training

Any employee with the ability to open a new account, or access/manage/close an existing account will receive training on identifying and detecting Red Flags. They will also be trained in the appropriate response actions in the event that an instance of identity theft is suspected. Key management personnel in appropriate departments will also receive training on the contents of this Program. As necessary, employees will be re-trained annually if the Program is updated to include new methods of identifying and detecting Red Flags, or if new response actions are implemented.

B. Program Review and Update

SJCUD will review and update the Program annually to reflect changes in risks to customers from identity theft based on factors such as:

- Experiences of SJCUD with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that SJCUD offers or maintains.
- Changes in the business arrangements of SJCUD, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

C. Program Approval and Adoption

This Program has been reviewed and approved by the St. Johns County Board of County Commissioners. SJCUD has assigned the Customer Service Manager to be responsible for the oversight, development, implementation and administration of the Program. Annually, the Customer Service Manager will develop the annual report as described in Section D that will address compliance of SJCUD with this Program. The St. Johns County Board of County Commissioners is responsible for reviewing this report and

approving material changes to the Program as necessary to address changing identity theft risks.

D. Annual Reporting

SJCUD will provide an annual report to the St. Johns County Board of County Commissioners that details SJCUD's compliance with the Federal Trade Commission's Red Flags Rule. The report will address matters related to the Program and address several topic areas including:

- Effectiveness of the policies and procedures of the Utility in addressing the risk of identity theft in connection with the opening of new accounts and with respect to the management of existing accounts;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and,
- Recommendations for material changes to the Program.

E. Service Provider Oversight

Whenever SJCUD engages a service provider to perform an activity in connection with one or more of the customer accounts, SJCUD will verify that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To accomplish this, SJCUD will require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to SJCUD, or to take appropriate steps to prevent or mitigate identity theft.