TO: James L. App, City Manager

FROM: Jim Throop, Director of Administrative Service

SUBJECT: Security Information Policy – "Red Flag"

DATE: October 21, 2008

NEEDS:

For the City Council to consider a formal policy on Identity Theft Protection as required by the Federal Trade Commission (FTC).

FACTS:

1. The FTC "Red Flag" Rules are federal regulations that are part of the Fair and Accurate Credit Transactions Act of 2003.

2. The Act requires financial institutions and creditors with covered accounts to design and implement a written identity theft prevention program by November 1, 2008.

3. The policies and procedures of the program must include the following four basic elements:

   i. Identify relevant warning signs, including patterns, practices, or specific activities, that are indicative of identity theft, i.e. "red flags";
   ii. Detect the red flags that have been incorporated into the program;
   iii. Provide for appropriate responses to such red flags in order to prevent or mitigate identity theft with respect to the covered account;
   iv. Detail a plan to periodically update the program.

4. The City of Paso Robles, by definition of the FTC, is considered a creditor due to our deferring of payment for goods and services from our customers, such as with our water and sewer utility billing.

5. The City's Utility Billing division has always been diligent in its security of personal identification, both computerized and in paper form.

6. The Administrative Services department will be required to prepare an annual report which addresses the effectiveness of the program, documents significant incidents involving identity theft and related responses, provides updates related to external service providers, and includes recommendations for material changes to the program. The Administrative Services Director approve the annual report.

ANALYSIS & CONCLUSION:

The FTC is requiring the formal adoption by City Council of a policy and procedure to deal with identity theft.

This requirement is for financial institutions and creditors. According to the FTC, since the City defers payment by its customers when water, electric, gas trash and the like are sold to customers day-by-day, but paid for at the end of the billing cycle, the City is a creditor.

The Administrative Services department will prepare annual report and the Administrative Services will accept and sign-off or accept with any recommended changes to the policy or program.

FISCAL IMPACT:

There is no financial impact on the City.

OPTIONS:

a. Adopt Resolution No. 08-xxx authorizing the approval of the Security Information Policy or "Red Flag" policy as required by the Federal Trade Commission..; or

b. Amend, modify or reject above option.

RESOLUTION NO. 08-____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF EL PASO DE ROBLES APPROVING AND ADOPTING THE IDENTITY THEFT PREVENTION PROGRAM AND POLICY FOR UTILITY ACCOUNTS

WHEREAS, pursuant to the Fair and Accurate Credit Transaction ("FACT") Act of 2003 issued by the Federal Trade Commission (the "FTC"), the City of El Paso de Robles (the "City Council") is required to adopt a program to help protect the personal and financial information of residents and businesses that have certain accounts with the City; and

WHEREAS the FACT Act requires that financial institutions and creditors implement written programs, which must be in place by November 1, 2008, that provide for the detection of and response to specific activities ("red flags") that could be related to identity theft; and

WHEREAS, the FTC requires that the program must: (1) identify relevant red flags and incorporate them into the program; (2) identify ways to detect red flags; (3) include appropriate responses to red flags; (4) address new and changing risks through periodic program updates; and (5) include a process for administration and oversight of the program; and

WHEREAS, the City of El Paso De Robles Finance Department, Utility Billing Services Division (the "Finance Department"), has prepared and presented to the City Council for approval an Identity Theft Prevention Program, which complies with the requirements of the FACT Act, as well as a Privacy of utility Account Information Policy, to help protect City utility customers; and

WHEREAS, the City Council desires to approve and adopt the Identity Theft Prevention Program and the Privacy of Utility Account Information Policy to provide for the detection of and response to specific activities that could be related to identity theft as required by the FACT Act;

NOW, THEREFORE, BE IT HEREBY RESOLVED that the City Council of the City of El Paso de Robles does hereby approve and adopt the Identity Theft Prevention Program in substantially the form attached hereto as Attachment A, and the Privacy of Utility Account Information Policy, attached hereto as Exhibit B, which are both incorporated herein by reference. The City Manager is hereby authorized and directed to take all actions and execute such other documents as may be necessary to implement and carry out the obligations of the City in accordance with the provisions of the Identity Theft Prevention Program, on behalf of the City Council.

PASSED AND ADOPTED by the City Council of the City of Paso Robles this ____ day of _____ 2008 by the following vote to wit:

AYES:

NOES:

ABSENT:

ABSTAIN:

_____
Mayor

ATTEST:

_____
City Clerk

Attachment A

City of El Paso De Robles

Finance Department

Utility Billing Services Division

Identity Theft Prevention Program

This program is in response to and in compliance with the

Fair and Accurate Credit Transaction (FACT) Act of 2003

and

The final rules and guidelines for the FACT Act issued by the Federal Trade Commission and federal bank regulatory agencies in November 2007

Adopted October XX, 2008 – Resolution # XX

Identity Theft Prevention Program

Purpose

This document was created in order to comply with regulations issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The FACT Act requires that financial institutions and creditors implement written programs which provide for detection of and response to specific activities ("red flags") that could be related to identity theft. These programs must be in place by November 1, 2008.

The FTC regulations require that the program must:

1. Identify relevant red flags and incorporate them into the program
2. Identify ways to detect red flags
3. Include appropriate responses to red flags
4. Address new and changing risks through periodic program updates
5. Include a process for administration and oversight of the program

Program Details

Relevant Red Flags

Red flags are warning signs or activities that alert a creditor to potential identity theft. The guidelines published by the FTC include 26 examples of red flags which fall into the five categories below:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers
- Presentation of suspicious documents
- Presentation of suspicious personal identifying information
- Unusual use of, or other suspicious activity related to, a covered account
- Notice from customers, victims of identity theft, or law enforcement authorities

After reviewing the FTC guidelines and examples, the Utility Billing Services Division determined that the following red flags are applicable to utility accounts. These red flags, and the appropriate responses, are the focus of this program.

- A consumer credit reporting agency reports the following in response to a credit check request:
    - Fraud or active duty alert
    - Credit freeze
    - The Social Security Number (SSN) is invalid or belongs to a deceased person
    - The age or gender on the credit report is clearly inconsistent with information provided by the customer
- Suspicious Documents and Activities
    - Documents provided for identification appear to have been altered or forged.
    - The photograph on the identification is not consistent with the physical appearance of the customer.
    - Other information on the identification is not consistent with information provided by the customer.
    - The SSN provided by the customer belongs to another customer in the Northstar System (NS).
    - The customer does not provide required identification documents when attempting to establish a utility account.
    - A customer refuses to provide proof of identity when discussing an established utility account.
    - A person other than the account holder or co-applicant requests information or asks to make changes to an established utility account.

- An employee requests access to the NS system or information about a utility account, and the request is inconsistent with the employee's need or ability to perform their official duties
- A customer notifies the Utility Billing Services Division of any of the following activities:
- Utility statements are not being received
- Unauthorized changes to a utility account
- Unauthorized charges on a utility account
- Fraudulent activity on the customer's bank account or credit card that is used to pay utility charges

- The Utility Billing Services Division is notified by a customer, a victim of identity theft, or a member of law enforcement that a utilities account has been opened for a person engaged in identity theft.

Detecting and Responding to Red Flags

Red flags will be detected as Utility Billing Services Division employees interact with customers and the City's credit reporting agency. An employee will be alerted to these red flags during the following processes:

- Establishing a new utility account: When establishing a new account, a customer is asked to provide a SSN or Driver License number so that in the event that an account goes into default, the Customer Service Representative (CSR) may submit the account to the proper collection service.

  Response: Do not establish the utility account. Ask the customer to appear in person and provide a government-issued photo identification. A deposit may also be required in order to establish service.

- Reviewing customer identification in order to establish an account or enroll the customer in the Direct Payment Plan (DPP) program: The CSRs may be presented with documents that appear altered or inconsistent with the information provided by the customer.

  Response: Do not establish the utility account or enroll the customer in the DPP until the customer's identity has been confirmed.

- Answering customer inquiries on the phone, via email, and at the counter: Someone other than the account holder or co-applicant may ask for information about a utility account (including Online BillPay accounts) or may ask to make changes to the information on an account. A customer may also refuse to verify their identity when asking about an account.

  Response: Inform the customer that the account holder or the co-applicant must give permission for them to receive information about the utility account. Do not make

changes to or provide any information about the account, with one exception: with one exception: if a person or agency makes payment on behalf of customer account

- Processing requests from City of Paso Robles employees: Employees may submit requests for information in the NS system that are inconsistent with the employee's need or ability to perform their official duties

Response: All requests for direct access to the NS system are approved by the Finance Manager, so the Information Technology Department should reject requests that have not received appropriate approval. All other requests for information from the NS system should be reviewed to ensure that they do not violate any part of the Privacy Policy. Requests that are inconsistent with the policy will be denied.

- Receiving notification that there is unauthorized activity associated with a utility account: Customers may call to alert the City about fraudulent activity related to their utility account and/or the bank account or credit card used to make payments on the account.

  Response: Verify the customer's identity, and notify the Administrative Coordinator immediately. Take the appropriate actions to correct the errors on the account, which may include:

  - Issuing a service order to connect or disconnect services
  - Assisting the customer with deactivation of their payment method (DPP)
  - Updating personal information on the utility account
  - Updating the mailing address on the utility account
  - Updating account notes to document the fraudulent activity
  - Notifying and working with law enforcement officials

- Receiving notification that a utilities account has been established for a person engaged in identity theft.

  Response: These issues should be escalated to the Administrative Coordinator immediately. The claim will be investigated, and appropriate action will be taken to resolve the issue as quickly as possible.

Additional procedures that help to protect against identity theft include:

- NS system access is based on the role of the user. Only certain job classifications have access to the entire system.
- The Finance Department will destroy paper receipts generated during credit card payment processing not less than 60 days after receipt is made.
- The Finance Department will ensure that service providers that receive and process utility billing information have programs in place to detect and prevent identity theft.

Administration and Oversight of the Program

Finance Department staff is required to prepare an annual report which addresses the effectiveness of the program, documents significant incidents involving identity theft and related responses, provides updates related to external service providers, and includes recommendations for material changes to the program.

The program will be reviewed at least annually and updated as needed based on the following events:

- Experience with identity theft
- Changes to the types of accounts and/or programs offered
- Implementation of new systems and/or new vendor contracts

Specific roles are as follows:

The Finance Manager (FM) will submit an annual report to the Administrative Services Director. The FM will also oversee the daily activities related to identity theft detection and prevention, and ensure that all members of the Utility Division staff are trained to detect and respond to red flags.

The FM will provide ongoing oversight to ensure that the program is effective.

The Administrative Services Director will review the annual report and approve recommended changes to the program, both annually and on an as-needed basis.

The City Council must approve the initial program.