Exhibit A

City of Lompoc

Finance Department

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 21st, 2008 – Resolution 5498(08)

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 Finance Department determined that the following red flags are applicable to utility and other 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 Customer Information System (CIS).
- The customer does not provide required identification documents when attempting to establish a utility, or other account, or make a payment.
- A customer refuses to provide proof of identity when discussing an established utility or other account.
- A person other than the account holder or co-applicant requests information or asks to make changes to an established utility or other account.
- An employee requests access to the CIS system or information about a utility or other account, and the request is inconsistent with the job duties and responsibilities of the employee.

- A customer notifies the Finance Department of any of the following activities:
  - Utility or other statements are not being received
  - Unauthorized changes to a utility or other account
  - Unauthorized charges on a utility or other account
  - Fraudulent activity on the customer's bank account or credit card that is used to pay utility and other charges
- The Finance Department is notified by a customer, a victim of identity theft, or a member of law enforcement that a utility or other 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 and Treasury or other City 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 or other account: When establishing a new account, a customer is asked to provide a SSN or other identification so that the Customer Service Representative (CSR) can run a credit check. Reports from the credit-reporting agency may contain red flags.

  Response: Do not establish the 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, process a payment, or enroll the customer in the automatic bank payment or credit card payment 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 account or accept payment 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 or other account (including Online 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 account. Do not make changes to or provide any information about the account, with one exception: if the service on the account has been interrupted for non-payment, the CSR may provide the payment amount needed for reconnection of service.

- Processing requests from City of Lompoc employees: Employees may submit requests for information in the CIS system that are inconsistent with their job duties and responsibilities.

  Response: All requests for direct access to the CIS system are approved by the Financial Services Manager, or his or her designee, so the Information Systems Department should reject requests that have not received appropriate approval. All other requests for information from the CIS 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 or other account: Customers may call to alert the City about fraudulent activity related to their utility or other 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 Financial Services Manager, or his or her designee, 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 automatic or other payment method
  - Updating personal information on the utility or other account

    - Updating the mailing address on the utility or other account
    - Updating account notes to document the fraudulent activity
    - Adding a password to the account
    - Notifying and working with law enforcement officials

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

  Response: These issues should be escalated to the Financial Services Manager, or his or her designee, 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:

- CIS system access is based on the role of the user. Only certain job classifications have access to the entire system.
- The Finance Department will investigate ways to reduce the number of paper receipts generated during credit card payment processing.
- 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 will 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 Financial Services Manager (FSM), or his or her designee, will submit an annual report to the Management Services Director. The FSM, or his or her designee, will also oversee the daily activities related to identity theft detection and prevention, and ensure that all members of the Finance Department, Utility Billing Division, Treasury Division and other appropriate City staff are trained to detect and respond to red flags.

The Financial Services Manager will provide ongoing oversight to ensure that the program is effective.

The Management 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.