



Meeting Date: 03/10/09

ACTION	TYPE OF ITEM
<input type="checkbox"/> Approved Recommendation	<input checked="" type="checkbox"/> Info/Consent
<input type="checkbox"/> Ord. No(s) _____	<input type="checkbox"/> Report
<input type="checkbox"/> Res. No(s) _____	<input type="checkbox"/> Public Hearing (Info/consent)
<input type="checkbox"/> Other _____	<input type="checkbox"/> Other _____

Prepared By: Danielle M. Navas

Agenda Item No. F-3

Reviewed By: City Manager *[Signature]*

City Attorney *[Signature]*

Finance *[Signature]*

Other (Specify) \_\_\_\_\_

**DATE:** February 17, 2009

**TO:** City Council

**FROM:** Danielle M. Navas, City Treasurer *[Signature]*

**SUBJECT:** Proposed Identity Theft Prevention Program

**RECOMMENDATION**

That City Council adopt the proposed Identity Theft Prevention Program.

**DISCUSSION**

The Fair and Accurate Credit Transactions Act of 2003 requires creditors, including utility providers, to develop and implement an Identity Theft Prevention Program by May 1, 2009. All organizations that extend credit to consumers, including utility service providers, must comply with this regulation which is intended to identify, mitigate and prevent identity theft.

The regulations require that the program:

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.

The program proposed by staff contains these five requirements and complies with the Fair and Accurate Credit Transactions Act of 2003.

**FINANCIAL IMPACT**

None at this time.

Attachment #1 – Identity Theft Prevention Program

**City of Oxnard  
City Treasurer's Office  
Utility Billing Division**

**Identity Theft Prevention Program**

This program is in response to and in compliance with the  
Fair and Accurate Credit Transactions (FACT) Act of 2003

and

The final rules and guidelines issued by the Federal Trade Commission,  
federal bank regulatory agencies and the National Credit Union  
Administration in November 2007

### **Purpose**

The purpose of this program is to comply with regulations issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The FACT Act requires that financial institutions and creditors implement procedures to detect and respond to specific activities that could be related to identity theft.

### **Definitions**

**Covered account** means:

1. Any account that a creditor offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions. Covered accounts include utility accounts; and
2. Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

**Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

**Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, review, or continue credit. A creditor includes a government entity that defers payment of goods or services.

**Identifying information** is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employment or taxpayer identification number, unique electronic identification number, computer's Internet Protocol (IP) address, or routing code.

**Identity Theft** means fraud committed or attempted using the identifying information of another person without authority.

**Red Flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

## **Program Details**

### **Identification of Relevant Red Flags**

The following events listed in the five categories below are considered red flags, which suggest that identity theft may be present:

- Alerts, Notifications, or Warnings From Credit Reporting Agencies
- Suspicious Documents
  - The documents provided for identification appear to have been altered, forged or inauthentic;
  - The photograph or physical description on the identification card is not consistent with the physical appearance of the customer;
  - Other document with information that is not consistent with existing information provided by the customer;
  - Application for service that appears to be forged.
- Suspicious Personal Identifying Information
  - Identifying information presented that is inconsistent with existing information provided by the customer;
  - Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
  - The driver's license number provided by the customer is the same as one given by another customer;
  - An address or phone number presented that is the same as that of another person;
  - A customer does not provide required identification documents when attempting to establish an account, make a payment or obtain information regarding the account;
  - A customer refuses to provide proof of identity when discussing an established account.
- Unusual Use of Account or Suspicious Account Activity
  - A person other than the account holder or co-applicant requests to make changes to an established account;
  - A person other than the account holder or co-applicant requests information or access to information stored in the CIS system, and the request is inconsistent with City Policy and customer privacy rights;
  - A customer informs City staff that utility statements have not been received;
  - A customer informs City staff of unauthorized changes or unauthorized charges to an account;
  - Change of address for an account followed by a request to change the account holder's name;
  - Mail sent to the account holder is repeatedly returned as undeliverable.

- Notices from Others
  - A customer notifies City staff of fraudulent activity on the customer's bank account or credit card that is used to pay utility charges;
  - City staff is notified by a customer, a victim of identity theft, or a member of law enforcement that an account has been opened or a fraudulent account is being maintained for a person engaged in identity theft.

### **Detection of Red Flags**

Red flags will be detected as City staff interacts with customers. Some of the red flags listed above will generally be detected when a person comes to the counter to open an account, pay for a service, or undertake another type of transaction. City staff should be ready to detect red flags at all times, including interactions that occur during the following processes:

- Establishing a new utility account;
- Reviewing customer identification to establish a new account or when accessing an existing account;
- Answering customer inquiries on the phone, via email, and at the counter;
- Processing requests from City of Oxnard employees, consultants and agents.

### **Response to Suspected Identity Theft**

In the event City staff detects any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

- Continue to monitor an account for evidence of identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Update personal information, mailing address and document the fraudulent activity
- Notify the Revenue Accounting Manager for determination of the appropriate step(s) to take;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

Additional procedures that help to protect against identity theft include:

- CIS system access will be based on the role of the user. Full access to the system will be allowed for certain positions only;
- Customers may access limited information about their utility account online and via the automated phone system. In order to access information online, customers must enroll using their utility account number and they must create a unique user identification and password;
- Ensure complete and secure destruction of paper documents and computer files containing customer information;

- Each department involved in financial transactions related to covered accounts will be provided with a copy of this policy;
- Employees, consultants and their agents requesting access or information from the CIS system will be required to sign an agreement to conditions on use of data.

### **Administration and Oversight of the Program**

Revenue Accounting Manager will prepare every two years a report to the City Treasurer which addresses the effectiveness of the program, documents significant incidents involving identity theft and related responses and includes recommendations for material changes to the program.

The program will be reviewed every two years and updated as needed based on the following events:

- Experience with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes to the types of accounts and/or programs offered or maintained;
- Implementation of new systems and/or new vendor contracts.

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