

RESOLUTION NO. 2008-719

Adopted by the Sacramento City Council

November 6, 2008

APPROVAL OF THE CITY OF SACRAMENTO UTILITY BILLING IDENTITY THEFT PREVENTION PROGRAM

BACKGROUND:

- A. The Federal Trade Commission (FTC) and Fair and Accurate Credit Transaction Act of 2003 has established Rules and Guidelines which require "creditors" having "covered accounts" to develop and implement an Identity Theft Prevention Program.
- B. Under these Rules and Guidelines, creditors must establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with any new or existing "covered accounts".
- C. The City of Sacramento Department of Utilities provides water, sewer, storm drain, and solid waste services to its residents, in which charges for services are billed after the services are provided, establishing the City as a "creditor" under the applicable FTC regulations. This requires the City to comply with the regulations by approving and implementing an identity theft prevention program.

BASED ON THE FACTS SET FORTH IN THE BACKGROUND, THE CITY COUNCIL RESOLVES AS FOLLOWS:

- Section 1. The City of Sacramento Utility Billing Identity Theft Program is set forth in Exhibit A is approved.
- Section 2. The City Manager or authorized designee is authorized to implement and administer the Program.

Table of Contents:

- Exhibit A: City of Sacramento Identity Theft Prevention Program

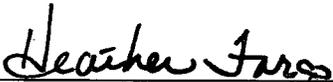
Adopted by the City of Sacramento City Council on November 6, 2008 by the following vote:

Ayes: Councilmembers Cohn, Fong, Hammond, McCarty, Pannell, Sheedy,
Tretheway, Waters, and Mayor Fargo.

Noes: None.

Abstain: None.

Absent: None.



Mayor Heather Fargo

Attest:



Shirley Concolino, City Clerk

CITY OF SACRAMENTO UTILTY BILLING IDENTITY THEFT PREVENTION
PROGRAM



City of Sacramento Utility Billing 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 November 6, 2008 – Resolution # XX

Identity Theft Prevention Program For Utility Billing

PURPOSE

The City of Sacramento has developed this Identity Theft Prevention Program for Utility Billing (the "Program") pursuant to the Federal Trade Commission's "Red Flags Rule" (Part 681 of Title 16 of the Code of Federal Regulations), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). The FACTA requires that financial institutions and creditors implement written programs that provide for identification, detection and response to patterns, practices or activities (called "red flags") that could be related to identify theft.

Under the Red Flags Rule, financial institutions and creditors are required to establish an identity theft prevention program tailored to their size and complexity and the nature and scope of their operations. After consideration of the size and complexity of the City's utility billing system, and the nature and scope of the City's utility billing operations, the Sacramento City Council has determined that this Program is appropriate for the City of Sacramento. As required by the Red Flags Rule, the initial Program has been approved by the City Council.

THE PROGRAM

Under the Red Flags Rule, the Program is required to include the following reasonable policies and procedures to detect, prevent, and mitigate identify theft:

1. Identify relevant red flags for covered accounts and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;
4. Ensure the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the City from identity theft; and
5. Provide for the continued administration of the Program.

The Program will, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks to customers or to the City of Sacramento from identity theft.

PROGRAM DEFINITIONS

The Red Flags Rule provides the following definitions of terms used in the Program:

Covered account means:

1. An 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, including financial, operational, compliance, reputation or litigation risks.

The City's utility service accounts are "covered accounts" under the Red Flags Rule.

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, renew, or continue credit. The Red Flags Rule defines a government entity that defers payment for goods or services as a creditor, for purposes of the Rule. By billing its customers for ongoing utility services after the services are provided, the City is a "creditor" under the Red Flags Rule.

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, employer 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.

IDENTIFICATION OF RELEVANT RED FLAGS

In order to identify relevant red flags, the City of Sacramento considers the types of utility service accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts and its previous experience with identify theft. The following red flags listed below within the five categories identified by the Federal Trade Commission are the red flags that could apply to the City's utility service accounts:

A. Notifications and Warnings From Credit Reporting Agencies

- Notice from a credit agency of a credit freeze on a customer; and
- Notice from a credit agency of an active duty alert for a customer.

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document; and
- Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged or ID does not match name on check or credit/debit card).

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with the information on record for the customer account;
- Identifying information presented that is inconsistent with other sources of information (for instance, a recorded deed or permit);
- Identifying information presented that is consistent with known fraudulent activity as indicated by internal or third-party sources;
- A mailing address provided is fictitious;
- A phone number provided is fictitious;
- A person refuses or fails to provide complete personal identifying information when contacting the City to discuss an established account; and
- A person other than the legal account holder or co-owner(s) requests information or asks to make changes to an established utility account.

D. Unusual Use of Account or Suspicious Account Activity

- Account used in a way that is not consistent with prior use (example: very high activity);
- The use of services that were disconnected or placed upon a vacancy stop;
- Service request is received on an inactive account or a parcel not being billed for City utility services.
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice is received indicating that a customer is not receiving paper statements or electronic bill notifications;
- Notice is received that an account has unauthorized activity or charges (such as a fee for a special service provided);
- Breach in the City's computer system security;
- Unauthorized access to or use of customer financial or account information; and
- An employee requests or obtains access to the City's Customer Information System (CIS) which is inconsistent with established policies and security measures for access.

E. Notice or Alerts from Others

- Notice to the City from a customer, victim of identity theft, law enforcement agency or other person that it has opened a fraudulent utility service account for a person engaged in identity theft;
- Notice to the City of fraudulent activity on a bank account or credit card that is used to pay for a customer's utility charges; and
- Notice from a customer of an illegal sale of a property.

DETECTION OF RED FLAGS

New Accounts

In order to detect any of the red flags identified above in connection with the opening of a new utility service account, the City's personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as legal owner(s) name, property address, residential or business mailing address, principal place of business for an entity, phone number and last four digits of a person's social security number;
- Verify the customer's identifying information with the recorded deed and mailing address from other sources (such as the County database);
- Review documentation showing the existence of a parcel, address, and/or business entity; and
- Independently contact the customer as necessary.

Existing Accounts

In order to detect any of the red flags identified above for an existing utility service account, the City's personnel will take the following steps to verify and monitor transactions on an account:

- Verify the identification of persons requesting account information matches the information on record for the legal owner(s), whether in person, via telephone, facsimile, mail or e-mail;
- Verify the identification of persons requesting changes to the bill mailing addresses matches the information on record for the legal owner(s); and
- Verify the identification of persons requesting changes to services matches the information on record for the legal owner(s).

RESPONSE TO SUSPECTED IDENTITY THEFT

In the event the City's personnel detect any identified red flags within any of the above red flag categories, such personnel will take one or more of the following steps depending on the degree of risk posed by the red flag:

A. Notifications and Warnings From Credit Reporting Agencies

- Contact the customer.

B. Suspicious Documents

- Not accept the payment method in which identifying information is questionable or inconsistent.
- Contact the issuing agency for a legal document or permit in question.

C. Suspicious Personal Identifying Information

- Not provide the requested information or changes.
- Contact the legal account holder(s).
- Require that the legal owner contact the City to continue with the request.
- Ask the customer to appear in person and provide government issued identification.

D. Unusual Use of Account or Suspicious Account Activity

- Perform an inspection at the property to validate occupancy.
- Use available resources to validate issuance of appropriate documents (i.e., permits, deeds)
- Contact the legal owner(s) of a property.
- Perform an investigation to validate information obtained or unauthorized activity.
- Use available resources to locate a valid mailing address for a person (such as skip trace).
- Change any passwords or other security devices that permit access to accounts.
- Reopen an account with a new account number.
- Notify law enforcement, or determine that no response is warranted under the particular circumstances.
- Deny unauthorized access to CIS.
- Take disciplinary action as appropriate for employees identified as misusing customer's financial or account information.

E. Notice or Alerts from Others

- Issue a service order to disconnect services.
- Notify the Program Administrator for determination of the appropriate step(s) to take.
- Notify and work with law enforcement.
- Conduct further investigation of the notice or alert.
- Remove account from automatic payment status, for a bank or credit card identified as being used fraudulently.
- Require submission of a police report and/or other supporting documentation for notification of illegal sales.

INTERNAL OPERATION PROCEDURES

In order to further prevent the likelihood of identity theft occurring with respect to utility service accounts, the City will take the following steps with respect to its internal operating procedures to protect customer identifying information:

- CIS system access requires a user based and/or job classification based role.
- Limited information can be accessed from the automated IVR.
- Online account management requires enrollment using a utility account number and service address and the creation of a unique user ID and password.
- Ensure that its website is secure or provide clear notice that the website is not secure.
- Ensure shredding of paper documents and computer files containing customer information.
- Ensure customer information on file is contained within a locked cabinet or password protected folders
- Ensure employees will not leave sensitive papers on their desks when they are away from their workstations.
- Ensure that the office computers are password protected and that computer screens lock after a set period of time.
- Keep offices clear of papers containing customer information.
- Request only the last 4 digits of social security numbers (if any).
- Ensure computer virus protection is up to date.
- Sensitive information that is sent to third parties over public networks will be encrypted.
- Require and maintain only the kinds of customer information that are necessary for utility purposes.
- Passwords will not be shared or posted near workstations
- The CIS database will timeout a session after a period of inactivity, requiring a password to access after timeout.
- The computer network will have a firewall where a network connects to the Internet.
- Ensure third party vendors maintaining or receiving customer information have security measures in places to prevent and mitigate identify theft.
- Store laptops in a secure place.
- If a laptop must be left in a vehicle, store in the trunk.

UPDATING THE PROGRAM

The Program will be reviewed and updated periodically as necessary to reflect changes in risks to customers or to the safety and soundness of the City of Sacramento from identity theft, based on factors such as:

- The experiences of the City with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;

- Changes in the types of covered accounts that the City offers or maintains for utility services;
- Changes in the City's business arrangements, such as service provider arrangements; and
- Implementation of new systems and/or vendor contracts.

ADMINISTRATION OF THE PROGRAM

- The Department Of Utilities Business Services Manager will be the Program Administrator primarily responsible for the development, implementation, oversight and continued administration of the Program.
- All staff handling utility service accounts will be trained, as necessary, to effectively implement the Program.
- Staff will be required to report all instances of fraudulent activity, documentation or notifications received to the Program Administrator or authorized designee.
- The Program will exercise appropriate and effective oversight of service provider arrangements.
- An annual report will be prepared on the effectiveness of the Program, including the number of red flag incidents and resolutions, and any recommended changes as a result of incidents or changes in the law, program operation, or methods or types of identity theft.
- The Director of Utilities will provide ongoing oversight to ensure the Program is effective.

OVERSIGHT OF THE PROGRAM

Oversight of the Program will include:

- a. Review of reports prepared by staff regarding compliance and incidents; and
- b. Approval of changes to the Program as necessary to address changing risks of identity theft.

Reports will be prepared as follows:

- a. On a regular periodic basis, designated staff involved in operation of the Program will provide a Program status report to the Business Services Manager including the information described in subsection (b) below.
- b. The report will document compliance with the Program and will evaluate issues such as:
 - The effectiveness of the Program in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - Service provider agreements;
 - Significant incidents involving identity theft and management's response; and
 - Any recommendations for changes to the Program.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

If the City engages a new service provider to perform an activity in connection with one or more utility service accounts, the City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

- Require, by contract, that service providers have such policies and procedures in place.
- Require, by contract, that service providers review the City's Program and report any red flags to the Program Administrator.

Existing contracted service providers will be required to submit documentation of security measures in place to prevent and mitigate identify theft.