Identity Theft Prevention

Program

Effective November 1, 2008

I. PROGRAM ADOPTION

The City of LaCenter ("Utility") operates and municipal wastewater collection and treatment system and developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule") codified at 16 CFR §681.2, which implements Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2003. This Program was developed with oversight by the Finance Director ("Program Administrator") and approved by the City of LaCenter City Council. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the City Council has determined that this Program was appropriate for the City of LaCenter, and therefore approved this Program on October 22, 2008.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing 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; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft." According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors." All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

"Identifying information" is defined under the Rule as "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 address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Utility considers the types of 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 experiences with Identity Theft. The Utility identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings From Credit Reporting Agencies, when used

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. An address or phone number presented that is the same as that of another person;
6. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the Utility from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. **New Accounts:** In order to detect any of the Red Flags identified above associated with the opening of a **new account**, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Review documentation showing the existence of a business entity; and/or
3. Independently contact the customer.

B. **Existing Accounts:** In order to detect any of the Red Flags identified above for an **existing account**, Utility personnel will take the following steps to extent possible to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility personnel detect Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Not open a new account;
4. Close an existing account;
5. Reopen an account with a new number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement; or
8. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of Identity Theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected;
4. Keep offices clear of papers containing customer information;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of customer information that are necessary for utility purposes.

VI. PROGRAM UPDATES

The Program Administrator will review and update this Program at least once a year to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. In doing so, the Program Administrator will consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight: Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the Utility. The Committee is headed by the Program Administrator or his or her appointee. One of the members should have detailed technical knowledge of the Utility's computer information systems. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports: Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected Utility staff will provide reports to the Program Administrator on incidents of Identity Theft. Department Heads are responsible to be familiar with the Identity Theft Protection Act and to meet with their staff to assess current compliance and document appropriate safeguard practices in writing.

C. Service Provider Arrangements: In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility 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.

1. Require that service providers have such policies and procedures in place; and
2. Require that service providers review the Utility's Program and report any Red Flags to the Program Administrator.

D. Non-disclosure of Specific Practices: For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to the Identity Theft Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "Security information" (as defined in the following paragraph) and are unavailable to the public because disclosure of them would be likely to substantially jeopardized the security of information against improper use, that use being to circumvent the Utility's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.

"Security information" is defined as government data the disclosure of which would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury.

City of La Center

214 East 4th Street, La Center, WA 98629
PHONE 360.263.8662 FAX 360.263.5700

SUMMARY OF RESOLUTION 08-303. A resolution an identity theft prevention program for use by the City's sewer utility. A complete text copy of Resolution 08-303 is available at La Center City Hall, 214 E. 4th St. This Resolution was passed by the City of La Center Council October 22, 2008, at a Regular Meeting/Public Hearing.

Suzanne Levis,
Finance Director/Clerk

Affidavit of Publication

STATE OF WASHINGTON)

) ss:

County of Clark)

Columbian

CATHY WINSTON
CITY OF LA CENTER-L
214 E FOURTH STREET
LA CENTER WA 98629

REFERENCE: 70243 IDENTITY THEFT POLIC
2957251 City of La Center 21

I, the undersigned say,

That I am over the age of eighteen and not interested in the above entitled matter; that I am now, and at all time embraced in the publication herein mentioned, was, the principal clerk of the printer of The Columbian, a daily newspaper printed, published and circulated in the said county and adjudged a newspaper of general circulation by the Superior Court of the County of Clark, State of Washington, under Proceeding No. 802006715; that the advertisement, of which the annexed is a true printed copy, was published in the above-named newspaper on the following dates, to wit:

City of La Center
214 East 4th Street
La Center, WA 98629
PHONE 360.263.8662
FAX 360.263.5700
SUMMARY OF RESOLUTION 08-303. A resolution an identity theft prevention program for use by the City's sewer utility. A complete text copy of Resolution 08-303 is available at La Center City Hall, 214 E. 4th St. This Resolution was passed by the City of La Center Council October 22, 2008, at a Regular Meeting/Public Hearing.
Suzanne Levis,
Finance Director/Clerk
Oct. 29 298204

PUBLISHED ON: 10/29

TOTAL COST: 33.00 AD SPACE: 20 LINE
FILED ON: 10/29/08

I Certify (or declare) under penalty of perjury that the foregoing is true and correct.

Signature Judy Moody