SULTAN CITY COUNCIL
AGENDA ITEM COVER SHEET

ITEM NO: Consent C 3

DATE: March 26, 2009

SUBJECT: Ordinance 1028-09 Red Flag Rules – Identity Theft Prevention

CONTACT PERSON: Laura Koenig, Clerk/Deputy Finance Director

ISSUE:
The issue before the Council is the adoption of Ordinance 1028-09 to establish an Identity Theft Prevention in compliance with the Federal Trade Commission's Fair and Accurate Credit Transaction Act of 2003. The ordinance was introduced for a first reading on March 12, 2009.

SUMMARY:
The Fair and Accurate Credit Transactions Act of 2003 requires certain financial institutions and creditors with "covered accounts" to prepare, adopt and implement an identity theft prevention program to provide identification of "red flags" that could indicate identity theft. Municipal utility accounts are specifically included under "covered accounts" and therefore the City will need to comply with the regulations.

The City is required to develop a program to identify, detect and respond to Red Flags, provide for a periodic updating process and a reporting process. There are five categories the City needs to address:

1. Notification from Consumer Reporting Agencies: The City does not request or receive information about its utility customers from any Consumer Reporting Agency.
2. Suspicious Documents: Documents that may be forged or altered.
3. Suspicious Personal Identifying Information: Identification that is not consistent with other personal information presented.
4. Unusual Use of or Suspicious Activity Related to an Account: Changes to account activity that is abnormal from prior history.
5. Notice Regarding Possible Identity Theft: This may come from a customer, victim or law enforcement officer.

These categories are addressed in the ordinance.

RECOMMENDED ACTION:
Adoption of Ordinance 1028-09 to establish an Identity Theft Prevention in compliance with the Federal Trade Commission's Fair and Accurate Credit Transaction Act of 2003..

Attachments: A) Ordinance 1028-09 – Identity Theft Prevention

ATTACHMENT A 1

CITY OF SULTAN
WASHINGTON

Ordinance 1028-09

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF SULTAN, WASHINGTON, APPROVING AND ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the City has a water-sewer utility providing water and/or sewer utility services pursuant to Title 57 RCW; and

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159 ("Red Flags Rule"), 16 C.F.R. Part 681, requires certain financial institutions and creditors with "covered accounts" to prepare, adopt, and implement an identity theft prevention program to identify, detect, respond to and mitigate patterns, practices or specific activities which could indicate identity theft; and

WHEREAS, the City maintains certain continuing accounts with utility service customers and for other purposes which involve multiple payments or transactions, and such accounts are "covered accounts" within the meaning of the Red Flags Rule; and

WHEREAS, to comply with the Red Flags Rule, City staff have prepared an identity theft prevention program in the form attached hereto as Exhibit "A" and incorporated herein by this reference (the "ITPP" or the "Program") and have recommended that the Program now be approved and adopted by the City Council for implementation;

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF SULTAN, WASHINGTON, DO ORDAIN AS FOLLOWS:

Section 1. The Program, as set forth in Exhibit "A," is hereby approved and adopted effective the date set forth below. City staff are hereby authorized and directed to implement the Program in accordance with its terms.

Section 2. Severability. Should any section, paragraph, sentence, clause or phrase of this Resolution, or its application to any person or circumstance, be declared unconstitutional or otherwise invalid for any reason, or should any portion of this Resolution be pre-empted by state or federal law or regulation, such decision or pre-emption shall not affect the validity of the remaining portions of this Resolution or its application to other persons or circumstances.

Section 3. Effective Date. This Ordinance shall be published in the official newspaper of the City, and shall take effect and be in full force five (5) days after the date of publication.

ATTACHMENT A 2

ADOPTED BY THE CITY COUNCIL AT A REGULAR MEETING THEREOF ON THE _____DAY OF _____, 2009.

CITY OF SULTAN

_____
Carolyn Eslick, Mayor

ATTEST/AUTHENTICATED:

_____
Laura Koenig, City Clerk
Approved as to form:

_____
Margaret J. King, City Attorney

Date of Publication:
Effective Date:

ATTACHMENT A 3

EXHIBIT 'A'

IDENTITY THEFT PREVENTION PROGRAM

PROGRAM ADOPTION

The City of Sultan developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with the oversight and approval of the City's Finance Director. After consideration of the size and complexity of the City's operations and account systems, and the nature and scope of the City's activities, the City Council determined that this Program was appropriate for the City, and therefore approved this Program by the adoption of Ordinance 1028-09 on the _____ day of _____, 2008.

PROGRAM PURPOSE AND DEFINITIONS

Fulfilling requirements of the Red Flags Rule

Under the Red Flags 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. The program must contain reasonable policies and procedures to:

- Identity relevant Red Flags as defined in the Rule and this Program for new and existing covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Update the Program periodically to reflect changes in risks to customers or to the safety and soundness of the District from identity theft.

Red Flags Rule definitions used in this Program

For the purposes of this Program, the following definitions apply:

Account. "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.
Covered Account. A "covered account" means:
Any account the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
Any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from Identity Theft.

Creditor. "Creditor" has the same meaning as defined in Section 701 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a, and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the City.
Customer. A "customer" means a person or business entity that has a covered account with the City.
Financial Institution. "Financial institution" means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a customer.
Identifying Information. "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identity a specific person, including name, address, telephone number, social security number, date of birth, government passport number, employer or taxpayer identification number or unique electronic identification number.
Identity Theft. "Identity Theft" means fraud committed using the identifying information of another person.
Red Flag. A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
Service Provider. "Service provider" means a person or business entity that provides a service directly to the City relating to or connection with a covered account.

IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft. The City identifies the following Red Flags, in each of the listed categories:

A. Notification and Warnings From Credit Reporting Agencies

Red Flags

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

B. Suspicious Documents

Red Flags

- 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;
-

- Other document with information that is not consistent with existing customer information (such as a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

- Identifying information presented that is inconsistent with other information the customer provides (such as inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a driver's license);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another customer;
- An address or phone number presented that is the same as that of another person;
- Failing to provide complete personal identifying information on an application when reminded to do so **(however, by law social security numbers must not be required)**; and
- Identifying information which is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

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

E. Alerts from Others

Red Flag

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

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,** City personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

- 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;
- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Review documentation showing the existence of a business entity; and
- Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account,** City personnel will take the following steps to monitor transactions with an account:

Detect Red Flags

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

PREVENTING AND MITIGATING IDENTITY THEFT

In the event City personnel detect 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:

A. Prevent and Mitigate Identity Theft

- Monitor a covered account for evidence of Identity Theft;
- Contact the customer with the covered account;
- Change any passwords or other security codes and devices that permit access to a covered account;
- Not open a new covered account;
- Close an existing covered account;
- Reopen a covered account with a new number;
- Not attempt to collect payment on a covered account;
- Notify the Finance Director for determination of the appropriate step(s) to take;

- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

B. <u>Protect Customer Identifying Information</u>

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

- Secure the City website but provide clear notice that the website is not secure;
- Undertake complete and secure destruction of paper documents and computer files containing customer information;
- Make office computers password protected and provide that computer screens lock after a set period of time;
- Keep offices clear of papers containing customer identifying information;
- Request only the last 4 digits of social security numbers (if any);
- Maintain computer virus protection up to date; and
- Require and keep only the kinds of customer information that are necessary for City purposes.

<u>PROGRAM ADMINISTRATION</u>

A. Oversight

The Finance Director or other designated city employee at the level of senior management shall be responsible for developing, implementing and updating the Program.

The Finance Director shall also be responsible for the Program administration, for appropriate training of City staff on the Program, for reviewing the annual staff report required under the Program, as well as any other 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

City staff responsible for implementing the Program shall be trained either by or under the direction of the Finance Director in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Additionally, a compliance report shall be provided annually to the Finance Director. The annual compliance report shall at a minimum address the following:

1. The effectiveness of the City's policies and procedures in addressing the risk of Identity Theft in connection with the opening of covered accounts and with respect to existing covered accounts;

2. Service provider arrangements;
3. Significant incidents involving identity theft and the City's response; and
4. Recommendations for material changes to the Program.

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more covered accounts, the City shall take the following steps to require that 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 acknowledge receipt and review of the Program and agree to perform its activities with respect to City covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Finance Director relative to the Program; or
- Require, by contract, that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to City covered accounts in compliance with the terms and conditions of the service provider's Identity Theft prevention program and will take appropriate action to prevent and mitigate Identity Theft; and that the service providers agree to report promptly to the City in writing if the service provider in connection with a City covered account detects an incident of actual or attempted Identity Theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.

D. Customer Identifying Information and Public Disclosure

The identifying information of City customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law, including RCW 42.56.230(4). The City Council also finds and determines that public disclosure of the City's specific practices to identity, detect, prevent and mitigate Identify Theft may compromise the effectiveness of such practices and hereby direct that, under the Program, knowledge of such specific practices shall be limited to the Finance Director and those City employees and service providers who need to be aware of such practices for the purpose of preventing Identity Theft.

PROGRAM UPDATES

The Program will be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the City from Identity Theft. The Finance Director shall at least annually review the annual compliance report and consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City's business arrangements with other entities and service providers. After considering these factors, the Finance Director shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Finance Director shall present the recommended changes to the City Council for review and approval.