RESOLUTION NO. 1148

A RESOLUTION OF THE CITY OF CAMAS,
WASHINGTON adopting an Identity Theft Prevention Program

WHEREAS, the City of Camas has developed an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, and

WHEREAS, the City Council has reviewed the Identity Theft Prevention Progam and has determined that the City's interest will be furthered by adoption of said program,

NOW, THEREFORE, be it resolved by the Council of the City of Camas as follows:

Section I

There is hereby adopted as the Identity Theft Prevention Program of the City, that document entitled "Identity Theft Prevention Program", a copy of which is attached hereto and by this reference incorporated herein.

ADOPTED by the Council at a regular meeting this 20th day of April, 2009.

SIGNED: _____
Mayor

ATTEST: _____
Clerk

APPROVED as to form:

_____
City Attorney

IDENTITY THEFT PREVENTION PROGRAM

I. PURPOSE

The City of Camas ("City") developed this Identity Theft Prevention Program (Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. & 681.2.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flag Rule

Under the Red Flag Rule, the City as a 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:

1. Identify relevant Red Flags for new and existing utility 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 the Program

The Red Flags Rule defines "identity theft" as a "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."

All the City's utility accounts whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the City maintains primarily for personal, family or household purposes, that involves multiple payments or transactions, and
2. Any other account the City maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City 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, date of birth, social security number, 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 City considers the types of accounts that it maintains, the methods it provides to open accounts, the methods it provides to access its accounts, and its previous experience with identity theft. The City identifies the following red flags, in each of the listed categories:

A. Suspicious Document

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.

B. 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 driver's license):
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 fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers will not be required); and
7. A person's identifying information is not consistent with the information that is on file for the customer.

C. Suspicious Account Activity or Unusual Use of Account

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 customer is repeatedly returned as undeliverable;
5. Notice to the City that a customer is not receiving mail sent by the City;
6. Notice to the City that an account has unauthorized activity;

7. Breach in the City's computer system security, and
8. Unauthorized access to or use of customer account information.

D. Alerts from Others

1. Notice to the City 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**, City 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 a name, date of birth, driver's license or other identification;
2. Verify the customer's identity with the customer (for instance, review a driver's license or date of birth):
3. Review documentation showing the existence of a business entity; and
4. 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

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 billing and payment purposes.

V. 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:

Prevent and Mitigate

1. Continue to monitor an account for evidence of identity theft;
2. Place "pop-up" warning in customer account;
3. Contact the customer;
4. Change any passwords or other security devices that permit access to accounts;
5. Not open a new account;
6. Close an existing account;
7. Reopen an account with a new number;
8. Enter Red Flag information into identity theft Prevention Log @ G:\FINANCE\Red Flag - Identity Theft Prevention Program\Red Flag Log.xls.
9. Notify the Finance Director for determination of the appropriate step(s) to take;
10. Notify the Police Department; or
11. 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 accounts, the City will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure complete and secure destruction of paper documents and computer files containing customer information;
2. Ensure that office computers are password protected and that computer screens lock after a set period of time of non-attendance;
3. Keep papers containing customer information locked in the Finance vault;
4. Ensure computer virus protection is up to date, and
5. Require and keep only the customer information that is necessary for City purposes.

VI. PROGRAM ADMINISTRATION & UPDATES

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Finance Director. The Finance Director will be responsible for the Program administration, for ensuring appropriate training of City staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, and determining which steps of prevention and mitigation should be taken in particular circumstances.

B. Staff Training and Reports

City staff responsible for implementing the Program shall be trained in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Training will be provided on a periodic basis and at the implementation of any new Program amendments.

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more accounts, the City will take the following steps to ensure the service provide 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 City's Program and report any Red Flags to the Finance Director.