

CITY OF SEQUIM
RESOLUTION NO. R-2009-05

A RESOLUTION ADOPTING AN IDENTITY THEFT POLICY

WHEREAS, the Identity Theft Prevention Program is designed to aid in the detection, prevention and mitigation of identity theft in connection with the opening of a Covered Account or an existing Covered Account; and

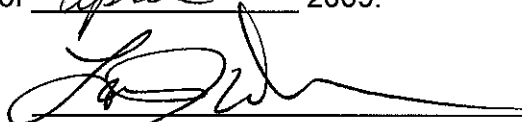
WHEREAS, the Identity Theft Prevention Program is to provide for continued compliance of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003; and

WHEREAS, the City of Sequim provides utility service to its citizens; and

WHEREAS, the City of Sequim maintains certain continuing accounts with utility service customers and for other purposes which involve payments or transactions.


NOW, THEREFORE, BE IT RESOLVED by the City Council that the policy attached as Exhibit A Identity Theft Policy, attached hereto, is hereby approved and adopted. Exhibit B outlines procedures to be followed, which may hereafter be amended.

Dated this 27th day of April 2009.



Laura Dubois, Mayor

Attest:



Karen Kuznek-Reese, CMC
City Clerk

Approved as to form:



Craig A. Ritchie, City Attorney



Administrative Policies

SUBJECT: IDENTITY THEFT PREVENTION POLICY	MANAGEMENT REVIEW DATE:	EFFECTIVE DATE: 4/27/09
---	--	--------------------------------

I. PURPOSE.

This Identity Theft Prevention Policy is designed to help prevent identity theft by appropriately securing "identifying information," to aid in the detection and mitigation of identity theft in connection with the opening of a "Covered Account" or an existing "Covered Account," and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

II. POLICY.

This policy applies to "covered accounts" maintained by the City.

Definitions

1. For purposes of this Program, the term "*Identity Theft*" means a fraud committed or attempted using the identifying information of another person without authority.
2. For purposes of this Program, the term "*Covered Account*" means (i) any account City offers or maintains primarily for personal family or household purposes, that involves multiple payments or transactions, including one or more deferred payments; and (ii) any other account the City identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of the City from Identity Theft. Currently utility customer accounts appear to be the only "covered accounts."
3. For purposes of this Program, the term "*Red Flag*" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
4. For purposes of this Program, the term "*Identifying Information*" means any name or number that may be used alone or with any other information to identify a specific person; this includes name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport, and employer or tax identification number.

The Program

This Program includes policies and procedures to:

1. Identify relevant red flags for covered accounts;
2. Define procedures on how to detect red flags, and how to prevent and mitigate identity theft when red flags are present.
3. Provide for continued administration of the Program.



Administrative Policies

Identification of Relevant Red Flags

The following events/occurrences reasonably indicate the potential for identity theft and are considered "Red Flags" for purposes of this program:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
2. The presentation of suspicious documents, such as:
 - a. Documents provided for identification appear to have been altered or forged.
 - b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
 - c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
 - d. Other information on the identification is not consistent with readily accessible information that is on file.
 - e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
3. The presentation of suspicious personal identifying information.
 - a. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range or date of birth.
 - b. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City of Sequim. For example:
 - i. The address on an application is the same as the address provided on a fraudulent application; or
 - ii. The phone number on an application is the same as the number provided on a fraudulent application.
 - c. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City of Sequim. For example:
 - i. The address on an application is fictitious, a mail drop, or a prison; or
 - ii. Phone number is invalid, or is associated with a pager or answering service.
 - d. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.



Administrative Policies

- e. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - f. Personal identifying information provided is not consistent with personal identifying information that is on file with the City of Sequim.
 - g. If the City of Sequim uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
4. The unusual use of, or other suspicious activity related to, a covered account:
- a. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
 - b. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - i. Nonpayment when there is no history of late or missed payments;
 - ii. A material increase in the use of available credit;
 - iii. A material change in purchasing or spending patterns;
 - c. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
 - d. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
 - e. The City of Sequim is notified that the customer is not receiving paper account statements.
 - f. The City of Sequim is notified of unauthorized charges or transactions in connection with a customer's covered account.
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the City of Sequim:
- a. The City of Sequim is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

III. PROCEDURE.

The procedures for prevention, detection and mitigation are outlined in Exhibit B, Procedures, which may hereafter be amended.



General Operating Procedures

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM			CHAPTER: PERSONNEL POLICIES
REVIEWED:	APPROVED:	<input checked="" type="checkbox"/> PERSONNEL <input type="checkbox"/> ADMINISTRATIVE – RESOLUTION _____	EFFECTIVE:

- I. PURPOSE.** To establish procedures for Prevention, Detection and Mitigation of Red Flags concerning identity theft.
- II. POLICY.** As adopted by Resolution No. R-2009-05.
- III. PROCEDURES.**

Detection, Prevention and Mitigation

1. **Detection:** In an effort to ensure proper detection of any Red Flags, all customers (consumers) must provide at least the following information/documentation before any new covered account will be opened:
 - a. Full Name;
 - b. Date of birth (individual);
 - c. Address, (a residential or business street address for an individual; for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual; or for a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and;
 - d. Identification number, which shall be: (i) For a U.S. person, a taxpayer identification number, social security number or government issued photo ID; or (ii) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

2. **Preventing and Mitigating Identity Theft:** In the event a Red Flag is detected, the City of Sequim will take reasonable steps to prevent the occurrence of identity theft to mitigate any harm caused thereby. In order to respond appropriately to the detection of a Red Flag, the City of Sequim shall consider any aggravating circumstance(s) that may heighten the risk of identity theft. After assessing the degree of risk posed, the City of Sequim will respond to the Red Flag in an appropriate manner, which may include:
 - a. Monitoring a covered account for evidence of identity theft;
 - b. Contacting the customer;
 - c. Changing any passwords, security codes, or other security devices that permit access to a covered account;



General Operating Procedures

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM		CHAPTER: PERSONNEL POLICIES
REVIEWED:	APPROVED:	<input checked="" type="checkbox"/> PERSONNEL <input type="checkbox"/> ADMINISTRATIVE – RESOLUTION _____
		EFFECTIVE:

- d. Reopening a covered account with a new account number;
- e. Not opening a new covered account;
- f. Closing an existing covered account;
- g. Notifying law enforcement; or
- h. Determining that no response is warranted under the particular circumstances.

3. Confidentiality of Applications and Account Information. All personal information, personal identifying information, account applications and account information collected and maintained by the City shall be a confidential record of the City and shall not be subject to disclosure unless otherwise required by State or Federal Law. Additionally, any employee with access to customers' personal information, account applications or account information shall maintain the confidentiality of such record. Employees are prohibited from copying or distributing confidential information. Employees who violate this provision shall be subject to discipline up to, and including, termination. Employees shall adhere to these requirements as well as those hereafter outlined in the City's employment handbook.

4. Access to Utility Account or Personal Identifying Information. Access to utility account information shall be limited to employees that provide customer service and technical support to the City's utilities. Any computer that has access to a customer utility account or personal identifying information shall be password protected (see City computer use policy for password standards) and all computer screens shall lock after no more than fifteen (15) minutes of inactivity. All paper and non-electronic based utility account or customer personal identifying information shall be stored and maintained appropriately and access shall only be granted by the System Administrator or his/her designee.

Record retention areas containing documents with sensitive identifying information will be stored when not in use. Desks, work areas, printers and fax machines will be cleared of all documents containing sensitive identifying information when not in use. Records will be disposed of in accordance with state and federal law. All electronically stored identifying information will be stored in a secure environment. Access into the system containing identifying information requires a password. The system will automatically disable the password after the designated number of unsuccessful login attempts. Only the System Administrator can reissue another password. Upon termination, employee passwords are immediately disabled.

5. Electronic Distribution. Each employee and contractor performing work for the City will comply with the following standards:



General Operating Procedures

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM			CHAPTER: PERSONNEL POLICIES
REVIEWED:	APPROVED:	<input checked="" type="checkbox"/> PERSONNEL <input type="checkbox"/> ADMINISTRATIVE – RESOLUTION _____	EFFECTIVE:

- a. Internally, sensitive information may only be transmitted using the approved email application and municipal email system. Additionally the message should be marked as confidential.
- b. Any sensitive information sent externally must be encrypted and password protected, and be sent only to approved recipients. Additionally, the message should be marked confidential and include a statement such as the following:

“This message may contain confidential and/or proprietary information and is intended for the person/entity to whom the message was originally addressed. Any use by others is strictly prohibited.”

6. **Updating the Program.** This Program shall be updated periodically to reflect changes in risks to customers of the City of Sequim from identity theft based on factors such as:
 - a. The experiences of the City of Sequim with identity theft;
 - b. Changes in methods of identity theft;
 - c. Changes in methods to prevent, detect and mitigate identity theft;
 - d. Changes in the types of accounts that the City of Sequim offers or maintains; or
 - e. Changes in the business arrangements of the City of Sequim, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

7. **Administration of the Program.** The City Clerk is responsible for implementation and administration of the Program. The City Clerk will report to Council at least annually on compliance by the City of Sequim with the Program. The report shall address material matters related to the Program and evaluate the effectiveness of the 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. The City Council will approve any material changes to the Policy as necessary to address changing identity theft risks.

8. **Oversight of Service Provider Arrangements.** The City of Sequim shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to prevent, detect and mitigate the risk of identity theft whenever the City of Sequim engages a service provider to perform an activity in connection with one or more covered accounts.



General Operating Procedures

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM			CHAPTER: PERSONNEL POLICIES
REVIEWED:	APPROVED:	(X) PERSONNEL () ADMINISTRATIVE – RESOLUTION _____	EFFECTIVE:

IV. ACKNOWLEDGEMENT.

This is to acknowledge that I have read and understand the City of Sequim's Policy.

Name: _____

Title: _____

Signature: _____

Date: _____