

RESOLUTION NO. 2009-12

A RESOLUTION OF THE CITY OF BELLINGHAM TO ADOPT A CITY IDENTITY THEFT PREVENTION PROGRAM PURSUANT TO FEDERAL LAW.

WHEREAS, the federal government enacted the Fair and Accurate Credit Transactions Act ("FACT Act") in 2003 amending the Fair Credit Reporting Act; and

WHEREAS, the FACT Act directed certain federal agencies, including the Federal Trade Commission ("FTC"), to issue regulations and guidelines to require certain "financial institutions and creditors", as defined by law to include utility companies, to establish an identity theft prevention program ("Program"); and

WHEREAS, the FTC's regulations and guidelines require that the Program should be designed to help detect, prevent, and mitigate identity theft to the extent practicable in connection with the opening or use of a utility account; and

WHEREAS, the FTC's regulations and guidelines were issued in 2008 with compliance mandated in May 2009; and

WHEREAS, the City Council has considered the size and complexity of the City's utility operations and account systems and the nature and scope of the City's relevant activities, and determines the attached Program is appropriate for the City;

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF BELLINGHAM:

THAT, the attached City of Bellingham Identity Theft Prevention Program is hereby approved and adopted.

PASSED by the Council this 27th day of April, 2009.



Council President

APPROVED by me this 15th day of May, 2009.



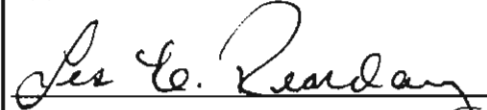
Mayor

Attest:



Finance Director

Approved as to form:



Office of the City Attorney

Published: n/a

CITY OF BELLINGHAM
IDENTITY THEFT PREVENTION PROGRAM

I. PROGRAM ADOPTION

The City of Bellingham ("City") operates certain utilities and other programs and has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule, as published in 16 Code of Federal Regulations Part 681 ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with approval of the City Council and the City's Finance Director ("Program Administrator"). After consideration of the size and complexity of the City's utility operations, other programs, and account systems, and the nature and scope of the City's relevant activities, the City Council determined that this Program was appropriate for the City, and therefore approved this Program by the adoption of Resolution No. 2009-12 on the 27th day of April, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. 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 designed to detect, prevent, and mitigate identify theft in connection with the opening of a covered account or an existing covered account to the extent practicable. The Program is to be 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 as defined in the Rule and this Program 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. Update the Program periodically to reflect changes in risks to customers or to the safety and soundness of the City from identity theft.

B. Red Flags Rule definitions used in this Program

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

1. 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.
2. Covered Account. A "covered account" means:
 - a. Any account the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
 - b. Any other account the City offers or maintains for which there is a reasonably

3. Creditor. "Creditor" has the same meaning as defined in Section 702 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.
4. Customer. A "customer" means a person or business entity that has a covered account with the City.
5. 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.
6. Identifying Information. "Identifying information" means 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 or unique electronic identification number.
7. Identity Theft. "Identity Theft" means fraud committed using the identifying information of another person.
8. Red Flag. A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
9. 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.

III. 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 (e.g. new and existing accounts), 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, by way of example, the following Red Flags, in each of the listed categories:

A. **Red Flags for Notifications and Warnings From Credit Reporting Agencies**

The City does not currently request credit reports but, to the extent, the City receives them, we will watch for:

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. **Red Flags for Suspicious Documents**

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 a person's signature on a check appears forged); and

C. Red Flags for Suspicious Personal Identifying Information

To the extent the City requests personal identifying information in relation to utility billing, we will look for:

1. Identifying information presented that is inconsistent with other information the customer provides (such as 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; and
6. Identifying information which is not consistent with the information that is on file for the customer.

D. Red Flags for 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 (such as very high activity);
4. Mail sent to the account holder 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.

E. Red Flags for Alerts from Others

1. 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.

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:

1. Require certain identifying information such as name, residential or business address, and/or principal place of business for an entity;
2. Review documentation showing the existence of a business entity; and

3. Independently contact the customer if we suspect identity theft or the information we have is otherwise inconsistent demonstrating suspicious activity.

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:

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 in the discretion of the City personnel detecting the Red Flag:

A. Prevent and Mitigate Identity Theft

1. Monitor a covered account for evidence of Identity Theft;
2. Contact the customer with the covered account;
3. Change any passwords or other security codes and devices that permit access to a covered account;
4. Not open a new covered account;
5. Close an existing covered account;
6. Reopen a covered account with a new number;
7. Not attempt to collect payment on a covered account;
8. Notify the Program Administrator for determination of the appropriate step(s) to take;
9. Notify law enforcement; or
10. Determine that no response is warranted under the particular circumstances.

B. Protect Customer Identifying Information

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

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

VI. PROGRAM UPDATES

The Program will be periodically reviewed and updated as may be needed to reflect changes in risks to customers and to the safety and soundness of the City from Identity Theft. In making such a review, the Program Administrator shall at least annually consider such factors as 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 Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall be authorized to update and implement the revised Program.

VII. PROGRAM ADMINISTRATION

A. Oversight

The Program Administrator shall be responsible for the Program administration, for 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, 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 Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. In the Program Administrator's discretion, City staff may submit periodic annual reports to the Program Administrator on such items as significant incidents of Identity Theft and the response, Program implementation and effectiveness, service provider arrangements, and 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. The City will require by contract that: (1) service providers review the Program; (2) acknowledge and verify they have similar policies and procedures in place or will follow the Program; and, (3) the service provider will report to the Program Administrator any Red Flags encountered during any activity in connection with one or more covered accounts while performing under the City contract.

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 extent authorized by law, including, by way of example, RCW 42.56.230 (Personal Information) and 42.56.330 (Public Utilities and Transportation), as currently enacted or hereafter amended. The City Council finds and determines that public disclosure of the City's specific practices to identify, detect, prevent and mitigate identity theft that may be developed and implemented under this Program may

and determines that public disclosure of the City's specific practices to identify, detect, prevent and mitigate identity theft that may be developed and implemented under this Program may compromise the effectiveness of such practices and hereby directs that, to the extent authorized by law, knowledge of such specific practices under this Program shall be limited to the Program Administrator and those City employees, agents, and service providers who need to be aware of such practices for the purpose of preventing Identity Theft.

E. No third party beneficiary.

This Program is intended to implement the FTC's Red Flag Rules by helping the City's covered programs identify suspicious behavior relating to potential identity theft. It is not intended to bestow any right, remedy or benefit on a third party nor is it intended to provide any cause of action or claim of any type against the City.