

**RESOLUTION NO. 2010-22**

**A RESOLUTION** of the City Council of the City of Bainbridge Island, Washington, approving and adopting an identity theft prevention program.

**WHEREAS**, the City of Bainbridge Island operates a consolidated waterworks utility providing water, sewer and storm and surface water management utility services pursuant to Title 13 of the City of Bainbridge Island Municipal Code and Title 57 of the RCW; and

**WHEREAS**, the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, ("Red Flag Rules") 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 with payment deferred until a future date and such accounts are "Covered Accounts" within the meaning of the Red Flag Rules; and

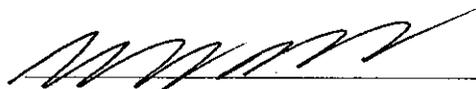
**WHEREAS**, to comply with the Red Flag Rules, the City has an identity theft prevention program in the form attached hereto as Exhibit "A" and incorporated herein by this reference (the "Program") and has recommended that the Program now be approved and adopted by the City Council for implementation; now, therefore,

**THE CITY COUNCIL OF THE CITY OF BAINBRIDGE ISLAND,  
WASHINGTON, DOES RESOLVE AS FOLLOWS:**

1. The Program is hereby approved and adopted effective as of the date set forth below.
2. The Finance Director is hereby authorized and directed to implement the Program in accordance with its terms.

PASSED by the City Council this 2<sup>nd</sup> day of June, 2010.

APPROVED by the Mayor this 2<sup>nd</sup> day of June, 2010.

  
\_\_\_\_\_  
Bob Scales, Mayor

ATTEST/AUTHENTICATE

Rosalind D. Lassoff  
Rosalind D. Lassoff, City Clerk

FILED WITH THE CITY CLERK: May 27, 2010  
PASSED BY THE CITY COUNCIL: June 2, 2010  
RESOLUTION NO. 2010-22

## EXHIBIT A

### Identity Theft Prevention Program

1. **Purpose.** To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate 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.

2. **Definitions.**

**Account** is defined as 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** is defined as (i) an account that a financial institution offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit, multiple payments or transactions, including one or more deferred payments; and (ii) any other accounts the City identifies as having a foreseeable risk to customers or to the safety and soundness of the City from identity theft.

**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.

**Customer** is a person or business entity that has a Covered Account with the City.

**Identifying information** means any name or number that may be used alone or with any other information to identify a specific person; including name, address, telephone number, social security number, date of birth, official state or government-issued driver's license or identification number, alien registration number, government passport, employer or tax identification number, and unique electronic identification number.

**Identity Theft** is defined as fraud committed using the identifying information of another person.

**Red Flag** is defined as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

**Service Provider** means a person or business entity that provides a service directly to the City relating to or connection with a Covered Account.

3. **The Program.** The City establishes an Identity Theft Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

- A. Identify relevant Red Flags for Covered Accounts that it offers or maintains and incorporate those Red Flags into the Program;
- B. Detect Red Flags that have been incorporated into the Program;
- C. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- D. Ensure that the Program is updated periodically to reflect any changes in risk to the customers and to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

4. **Identification of Red Flags.** The Program shall include relevant Red Flags from the following categories as appropriate:

- A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- B. The presentation of suspicious documents;
- C. The presentation of suspicious personal identifying information;
- D. The unusual use of, or other suspicious activity related to, a Covered Account; and
- E. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts.

The Program shall consider the following risk factors in identifying relevant Red Flags for Covered Accounts as appropriate:

- A. The types of Covered Accounts offered or maintained;
- B. The methods provided to open Covered Accounts;
- C. The methods provided to access Covered Accounts; and
- D. Any previous experience with identity theft.

The Program shall incorporate relevant Red Flags from sources such as:

- A. Incidents of identity theft previously experienced;
- B. Methods of identity theft that reflect changes in risk; and

C. Applicable supervisory guidance.

5. **Identification of Red Flags.** The City identifies the following Red Flags and will train the appropriate staff to recognize these Red Flags as they are encountered in the ordinary course of City business:

A. Suspicious documents

- i. Identification document or card that appears to be forged, altered or unauthentic;
- ii. Identification document or card where a person's photograph or physical description is not consistent with the person presenting the document;
- iii. Other information on the identification document is not consistent with the information provided by the person opening a new Covered Account, by the customer presenting the identification, or with existing customer information on file with the creditor (such as a signature card or recent check); and
- iv. Application for service that appears to have been altered or forged.

B. Suspicious personal identifying information

- i. Identifying information presented that is inconsistent with other information that the customer provides, for instance, where there is lack of correlation between the social security number range and the date of birth;
- ii. Identifying information presented that is inconsistent with external sources of information, for instance, and address does not match a consumer report or a social security number is listed in the Social Security Administration's Death Master File;
- iii. Identifying information presented is associated with common types of fraudulent activity, such as presentation of an invalid phone number or fictitious billing address used in previous fraudulent activity;
- iv. Social security number presented is the same number that has been given by another customer;
- v. An address or phone number presented that is the same as that of another person;

- vi. A person fails to provide complete personal identifying information on a application when reminded to do so (however, by law, social security numbers must not be required); and
- vii. 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 an account

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

D. Alerts from others

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

E. Notifications and Warnings From Credit Reporting Agencies

- i. Report of fraud accompanying a credit report;
- ii. Notice or report from a credit agency of a credit freeze on a customer or applicant;

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

6. **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 staff will take the following steps to obtain and verify the identity of the person opening the account:

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

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

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

7. **Preventing and Mitigating Identity Theft.** In the event that City staff detect any identified Red Flags, such staff must contact the City's Finance Director. The Finance Director will then decide which of the following steps should be taken:

- A. Monitor the Covered Account for evidence of identity theft;
- B. Contact the customer;

- C. Change any passwords, security codes, or other security devices that permit access to a Covered Account;
- D. Reopen a Covered Account with a new number;
- E. Not open a new Covered Account;
- F. Close an existing Covered Account;
- G. Notify law enforcement; or
- H. Determine that no response is warranted under the particular circumstances.

8. **Protect Customer Identifying Information.** 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:

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

9. **Program Updates.** The Finance Director, or designee, shall serve as the Program Administrator. The Program Administrator will periodically review and update this Program to reflect changes in risk to customers or to the safety and soundness of the organization from identity theft based on factors such as:

- A. The experiences of the City 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 offers or maintains; or
- E. Changes in the business arrangements of the City, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

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 recommended changes, and the City Council will make a determination of whether to accept, modify, or reject those changes to the Program.

10. **Administration of the Program.**

- A. The Program Administrator shall be responsible for the development, implementation, oversight, and continued administration of the Program;
- B. The Program shall include staff training, as necessary, to effectively implement the Program.
- C. The Program shall include appropriate and effective oversight of service provider arrangements.

11. **Oversight of the Program.** Oversight of the Program shall include:

- A. Implementation of the Program;
- B. Review of reports prepared by staff regarding compliance;
- C. Approval of material changes to the Program as necessary to address changing risks of identity theft.

Reports shall be prepared as follows:

- A. The staff responsible for development, implementation and administration of the Program shall report to the Program Administrator annually, at least, regarding compliance by the organization to the Program.
- B. The report shall include matters related to the Program such as:
  - i. The effectiveness of the policies and procedures in addressing the risk of identity theft as it relates to the opening of Covered Accounts and existing Covered Accounts;
  - ii. Service provider agreements;

- iii. Significant incidents involving identity theft and management's response.
- iv. Recommendations for material changes to the Program.

12. **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:

- A. 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 Program Administrator relative to the Program; or
- B. 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.

13. **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 identify, detect, prevent and mitigate identify theft may compromise the effectiveness of such practices and hereby directs that, under the Program, knowledge of such specific practices shall be limited to the Program Administrator and those City employees and Service Providers who need to be aware of such practices for the purpose of preventing Identity Theft.