RESOLUTION R-4754

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF KIRKLAND APPROVING AND ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM.

WHEREAS, Federal Trade Commission has issued regulations ("the Red Flags Rules") requiring financial institutions and creditors to develop and implement identity theft prevention programs under the Fair and Accurate Credit Transaction Act of 2003 ("FACTA"); and

WHEREAS, municipal utilities are subject to the Red Flags Rules; and

WHEREAS, the city councils of all cities that operate utilities must adopt programs that meet the Red Flags Rules of FACTA; and

WHEREAS, these programs must be in place by May 1, 2009, and must provide for the identification, detection and response to patterns, practices or specific activities known as "red flags" that could indicate identity theft; and

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

WHEREAS, to comply with the Red Flags Rules, City staff have prepared an identity theft prevention program and have recommended that the program now be approved and adopted by the City Council for implementation.

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

Section 1. The City Manager is hereby authorized and directed to implement the Identity Theft Prevention Program substantially similar to the form attached hereto as Exhibit "A" and incorporated herein by this reference in accordance with its terms.

Passed by majority vote of the Kirkland City Council in open meeting this 7th day of April, 2009.

Signed in authentication thereof this 7th day of April, 2009.

MAYOR

Attest:

City Clerk

IDENTITY THEFT PREVENTION PROGRAM

I. PROGRAM ADOPTION

The City of Kirkland ("City") 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. 16 C.F. R. §681.2. 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 Deputy Finance Director determined that this Program was appropriate for the City. The City Council approved this Program by the adoption of Resolution No. R-4754 on the seventh 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" tailored to the size, complexity and nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags 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. Ensure the Program is updated 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 reasonable foreseeable risk to customers or to the safety and soundness of the City from Identity Theft.

3. Creditor. "Creditor" has the same meaning as defined in Section 702 of the Equal Credit Opportunity Act, 15 US.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, computer Internet Protocol address, or routing code.

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 in connection with a covered account.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City considers the types of covered accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The City identifies the following Red Flags and will train appropriate staff to recognize these Red Flags as they are encountered in the ordinary course of City business:

A. Suspicious Documents

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 a signature card or recent check);
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;
2. Identifying information presented that is inconsistent with external sources of information, for instance, an address does not match 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 use of a fictitious billing address or invalid property owner's name;
5. An address or phone number presented that is the same as that of another person;
6. A person fails to complete personal indentifying information on an application when reminded to do so; 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

Red Flags

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 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 than 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

Red Flags

Notice to the City from a customer, identity theft victim, 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 staff will take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

1. Verify property ownership with King County parcel records;
2. Obtain certain identifying information such as name, phone number, residential or business address, principal place of business for an entity, driver's license or other identification; and
3. Verify the customer's identity, for instance, review a driver's license or other identification card.

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:

Detect Red Flags

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email); and
2. Verify that information on the account matches information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event City staff detect any identified Red Flags, the Deputy Finance Director will then decide which of the following steps should be taken:

Prevent and Mitigate Identity Theft

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security codes and devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify law enforcement; or
8. 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 City accounts, the City shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that the City website is secure or provide clear notice that the website is not secure;

2. Undertake complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are 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. Maintain up to date computer virus protections; and
6. Require and keep only the kinds of customer information that are necessary for City purposes.

VI. PROGRAM UPDATES

The Deputy Finance Director shall serve as Program Administrator. The Program Administrator shall periodically review and update this Program to reflect changes in risks to customers and the safety and soundness of the City from Identity Theft. In doing so, the Program Administrator shall, at least annually, consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, 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 update and implement the revised Program and present the recommended changes to the City Manager for review and approval.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator. The Program Administrator shall be responsible for the Program administration, for appropriate training of City staff, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, for determining which steps of prevention and mitigation should be taken in particular circumstances, and for 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. The Program Administrator will provide annual status reports to the City Manager regarding the City's compliance with the Program; the effectiveness of the Program with respect to opening accounts, existing covered accounts, and service provider arrangements; significant incidents involving Identity Theft and responses; and recommendations for 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 accounts, the City shall take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

1. Require that the service provider has such policies and procedures in place and that the service provider must 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
2. Require that service provider reviews the City's Program and report any Red Flags to the Program Administrator. Furthermore, the City shall require that the service provider 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 identify, detect, prevent, and mitigate Identity 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 staff and service providers who need to be aware of such practices for purpose of preventing Identity Theft.