Resolution No. 09-593

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF BLACK DIAMOND, KING COUNTY, WASHINGTON, AUTHORIZING AND ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM (KNOWN AS THE "RED FLAG PROGRAM") TO COMPLY WITH THE FAIR & ACCURATE CREDIT TRANSACTIONS ACT OF 2003

WHEREAS, the City of Black Diamond operates water, sewer, and storm water utilities; and

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, Pub. L.108-159, ("Red Flags Rule"), requires creditors who maintain "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 accounts for other purposes which involve multiple payments or transactions, and such accounts are "covered accounts" within the meaning of the Red Flags Rule; and

WHEREAS, to comply with the Red Flags Rule, City staff have prepared the attached Identity Theft Prevention Program which staff recommends be approved and adopted by the City Council for implementation.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF BLACK DIAMOND DOES RESOLVE AS FOLLOWS:

Section 1. The City of Black Diamond hereby authorizes and adopts an Identity Theft Prevention Program as described in Exhibit "A" to this Resolution and which is hereby incorporated to this Resolution by reference.

Section 2. The city's Identity Theft Program shall be administered by the City Finance Director, or his or her designee, and shall go into effect upon passage of this Resolution. The Finance Director shall periodically review the program and, in consultation with the City Administrator, update and amend the program as needed to enhance its continuing effectiveness. Such updates and amendments need not be reviewed and approved by the City Council, provided, the written policies and procedures being adopted by this Resolution must be updated whenever any future changes are made to the Program.

RESOLVED this 23rd day of April, 2009.

CITY OF BLACK DIAMOND

Mayor Howard Botts

ATTESTED BY:

Brenda L. Streepy, City Clerk

DATE OF PASSAGE BY THE CITY COUNCIL: 4/23/09

DATE OF FILING WITH THE CITY CLERK: 4/24/09

City of Black Diamond
Identity Theft Prevention Program

May 2009

CITY OF BLACK DIAMOND IDENTITY THEFT PREVENTION PROGRAM

Effective: May 2009
Policy Applies To: This policy applies to any account the City offers or maintains that involves multiple payments or transactions

I. PROGRAM ADOPTION

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

"Red Flags" shall mean any fact, behavior, or activity related to a customer's covered utility account that would cause a reasonable city employee to believe possible improper activity may be occurring. Although this policy gives examples of typical "red flags," city employees should not feel they are limited to only these types of occurrences and should use their training, experience, and common sense in bringing suspicious activity to the attention of the Finance Director.

II. CONFIDENTIALITY OF SPECIFIC PROGRAM PRACTICES

To promote effective Identity Theft prevention programs, the Red Flag Rule envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to Management and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation, and prevention practices are listed in this document.

III. THE CITY IS A "CREDITOR" UNDER THE LAW

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to the organization's size, complexity and the nature of its operation. According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors." In addition, the City of Black Diamond also falls under the Rule because the City maintains certain continuing accounts with utility service customers and accounts for other purposes which involve multiple payments or transactions.

IV. GOALS OF THE PROGRAM

The City's ID Theft Prevention 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 creditor from identity theft.

V. DEFINITIONS

"Covered account" means any individual utility service accounts held by customers of one or more of the City's utilities, whether residential, commercial, or industrial, including:

1. Any account the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

2. Any other account the City offers or 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" 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, unique electronic identification number, computer Internet Protocol address, or routing code.

VI. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City shall consider the types of 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, in each of the listed categories:

A. Notifications and Warnings From Credit Reporting Agencies

Red Flags:
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;
4) Notice or report from a credit agency of an address discrepancy; and

5) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags:

I) 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.

C. 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 credit report);
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. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. 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 (example: very highactivity);
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. Alerts from Others

Red Flags:

I. 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.

VII. 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 shall take the following steps to obtain and verify the identity of the person opening the account:

1. 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;

2. Verify the customer's identity (for instance, review a driver's license or other identification card);

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 staff shall take the following steps to monitor transactions with an account:

1. Verify the identity 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.

VIII. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility 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. Contact the customer;
3. Change any passwords or other security 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 the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information:

In order to 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 its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Not use social security numbers as a customer ID #
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for City purposes.

IX. PROGRAM UPDATES.

This Program will be periodically reviewed and updated to reflect changes in risks to customers and to improve the effectiveness of the program in preventing Identity Theft. The Finance Director, in consultation with the City Administrator, shall consider the City's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in the types of accounts the City maintains, and changes in the City's business arrangements with other entities. After considering these factors, the Finance Director shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Finance Director shall update these written Policies and Procedures to reflect any changes and implement the revised Program.

X. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for implementing and updating this Program lies with the Finance Director. The Finance Director will be responsible for the following: administering the program; developing procedures to implement the Program policies; ensuring appropriate training of City staff on the Program; reviewing 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; considering periodic changes to the Program.

B. Staff Training and Reports

City staff handling processing of utility accounts shall be trained either by or under the direction of the Finance Director in the detection of Red Flags, and about the steps to be taken when a Red Flag is detected. City staff shall prepare a report at least annually for the Finance Director, including an evaluation of the effectiveness of the Program with respect to opening accounts, existing covered accounts, service provider arrangements, any incidents involving identity theft and responses, and any recommendations for changes to the Program.

C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will 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, including:

1. Require, by contract, that service providers have such policies and procedures in place; and

2. Require, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator.

XI. SPECIFIC DUTY TO KEEP FINANCIAL ACCESS NUMBERS CONFIDENTIAL

The identifying information of the 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). Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers, shall not be released except when disclosure is expressly required by or governed by law.