CITY OF REDMOND
RESOLUTION NO. 1293

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDMOND, WASHINGTON, ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM PURSUANT TO THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

WHEREAS, the municipal utilities of the City of Redmond are considered "creditors" under the Fair and Accurate Credit Transaction Act of 2003 (Act), and

WHEREAS, the municipal utilities of the City of Redmond extend "credit," as defined in the Act, by deferring payment for services rendered, and

WHEREAS, the municipal utilities of the City of Redmond maintain "covered accounts", as defined in the Act, and

WHEREAS, the City of Redmond may also act as a "creditor" maintaining "covered accounts" in certain non-utility contexts requiring compliance with the Red Flag Rules, and

WHEREAS, the City of Redmond desires to adopt a policy establishing an Identity Theft Prevention Program pursuant to the Act

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF REDMOND, WASHINGTON, HEREBY RESOLVE AS FOLLOWS

Section 1 Adoption of the Identity Theft Prevention Program The City of Redmond's procedures for identifying, detecting, and responding to identity theft, attached hereto as

Exhibit 1 and adopted by this reference as if set forth in full, are hereby adopted for use by the City of Redmond to the full extent consistent with state law

ADOPTED by the Redmond City Council this 21st day of April, 2009

CITY OF REDMOND

MAYOR, JOHN MARCHIONE

ATTEST

MICHELLE M MCGEHEE, CMC, CITY CLERK (SEAL)

FILED WITH THE CITY CLERK April 15, 2009
PASSED BY THE CITY COUNCIL April 21, 2009
EFFECTIVE DATE April 21, 2009
RESOLUTION NO 1293

APPROVED 7-0 Allen, Carson, Cole, Margeson, McCormick, Myers and Vache

City of Redmond

Identity Theft Prevention Program

Effective beginning May 1, 2009

I PROGRAM ADOPTION

The City of Redmond developed this Identity Theft Prevention Program ("Program') pursuant to the Federal Trade Commission's Red Flag Rule ("Rule"), which implements Section 114 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 City Council determined that this Program was appropriate for the City of Redmond, and therefore adopted this Program on April 21, 2009

II PROGRAM PURPOSE AND DEFINITIONS

A Fulfilling requirements of the Red Flags Rule

Under the Red Flag 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 creditor from Identity Theft

B Red Flags Rule definitions used in this Program

The Red Flag Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft "

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 "

All the City's accounts that are individual utility service accounts held by customers of the City whether residential, commercial or industrial are covered by the Rule

In addition, the City may maintain certain "covered accounts" and act as a "creditor" in certain non-utility contexts The Rule defines "covered accounts ' as consumer accounts offered primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions For example, the City of Redmond maintains accounts to

accept payments for public defender services In these situations where the City maintains a covered account and accepts payment after a service is rendered, this Identity Theft Prevention Program will also apply

Under the Rule, a "covered account" is

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" is defined under the Rule as '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's Internet Protocol address, or routing code

III IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City considers 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 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 information on identification document is not consistent with 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
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,
3 Identifying information presented is associated with common types of fraudulent activity, such as use of a fictitious billing address or phone number,
4 Identifying information presented that is consistent with known fraudulent activity, such as presentation of an invalid phone number or fictitious billing address used in previous fraudulent activity,
5 An address or phone number presented that is the same as that of another person,
6 A person fails to provide complete personal identifying 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 (example 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

D Alerts from Others

Red Flag

1 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

IV PREVENTING AND MITIGATING IDENTITY THEFT

In the event City personnel detect any identified Red Flags, such personnel must contact the Finance Director of the City and/or designee The Finance Director and/or designee will then decide which of the following steps should be taken

a Contact the customer of any potential risk, whenever it is possible to do so,

b May request the customer to provide the City with proper picture identification in person to validate his identity,
c Report any Red Flags to the Program Administrator and/or designee,
d Continue to monitor an account for evidence of Identity Theft,
e Determine not to open a new account or close an existing account,
f Notify law enforcement, or
g Determine that no response is warranted under the particular circumstances

City personnel will also take the following steps to prevent identity theft

1 City staff will not discuss the utility account with anyone but the account holder or at the account holder's request Based on the recorded information in the billing system, staff will validate the identity of the account holder prior to discussing the utility account
2 A written request for access to the utility customer information must be submitted via e-mail to '_Utility Billing for internal request or by completing the City's Public Disclosure Request form through the City Clerk's office Customer information exempt from public disclosure (RCW 42 56 330) will not be disclosed to the maximum extent authorized by law
3 For credit card transactions, paper receipts to the utility customer will only contain the last 4 digits of the credit card number Any paper documents regarding credit card payment will be secured in the vault or shredded after payment has been processed by the Cashier
4 A customer's personal data will be either stored in a secured, locked cabinet or shredded immediately
5 Documents stored electronically will be maintained under a secured network drive with limited access
6 Office computers must be password protected and computer screens are to be locked when not in use
7 The utility billing systems are based on the role of the user All requests for access to the billing system must be submitted to the Revenue Manager and/or the Program Administrator for approval
8 The City will obtain and keep minimal customer information required for City purposes
9 City staff will advise utility customers not to use the unsecured email system to send personal information
10 City staff will report any Red Flags to the Program Administrator and/or designee
11 If a customer informs the City of any suspicious activities or possible identity theft problems, City staff will place a "warning" comment on an account and the alert message will pop-up whenever the account is opened or accessed by staff

V PROGRAM UPDATES

The Finance Director and/or designee shall serve as Program Administrator The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the City from Identity Theft In doing so, the Program Administrator and/or designee will consider the City's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the City's business arrangements with other entities After considering these factors, the Program Administrator and/or designee will determine whether changes to the Program, including the listing of Red Flags, are warranted If warranted, the Program Administrator and/or designee will update the Program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program

VI PROGRAM ADMINISTRATION

A Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator and/or designee The Program Administrator and/or designee will be responsible for the Program's administration, for ensuring 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 and/or designee in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected Staff should prepare a report at least annually for the Program Administrator and/or designee, including an evaluation of the effectiveness of the Program with respect to opening accounts, existing covered accounts, 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 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

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 and/or designee