RESOLUTION NO. 08-36

A RESOLUTION APPROVING A CITY OF KLAMATH FALLS POLICY ON IDENTITY THEFT PREVENTION AND RED FLAG ALERTS IN COMPLIANCE WITH FEDERAL AND STATE LAWS

WHEREAS, during the course of providing services to the citizens of this community, the City frequently comes into possession of personal, confidential information provided by customers and employees; and

WHEREAS, the City of Klamath Falls recognizes and takes seriously its responsibility to protect and safeguard the security, confidentiality and integrity of personal information entrusted to the City by its customers and employees; and

WHEREAS, the Federal Trade Commission has adopted "Red Flag" regulations under the Fair and Accurate Credit Transaction Act provisions of the Fair Credit Reporting Act; and

WHEREAS, these Red Flag rules require that by November 1, 2008 the City, as a utility provider, must adopt rules for identifying and detecting "red flags" that raise concerns about whether account information is potentially being misused or stolen; and

WHEREAS, the State of Oregon has passed the Oregon Consumer Identify Theft Protection Act, which requires that any entity, including a city, that holds certain types of personal information must protect and safeguard personal identifying information (including Social Security Numbers and other government issued numbers) and must notify consumers and employees in the event a breach of security compromises that information; and

WHEREAS, City staff has drafted a proposed policy that complies with the requirements of the federal Red Flag regulations and Oregon's Identity Theft Protection Act; and

WHEREAS, the City Council has determined that the proposed "Policy on Identity Theft Prevention and Red Flag Alerts" complies with federal and state law and will be a valuable tool for protecting personal, confidential information and deterring incidents of identity theft; NOW, THEREFORE.

THE CITY OF KLAMATH FALLS RESOLVES AS FOLLOWS:

Section 1.

Based on the foregoing recitals, which are adopted as findings herein, the City of Klamath Falls hereby approves and adopts the attached "Policy on Identity Theft Prevention and Red Flag Alerts."

Section 2.

The City Manager is hereby authorized: to implement said Policy; to create an Identity Theft Committee to monitor identify theft issues and propose changes to the Policy; and to amend the Policy as deemed appropriate.

Section 3.

This Resolution shall become effective immediately upon enactment.

Passed by the Council of the City of Klamath Falls, Oregon, the 20th day of October, 2008.

Presented to the Mayor, approved and signed this 21st day of October, 2008.

Mayor

ATTEST:

Deputy Recorder

STATE OF OREGON)
COUNTY OF KLAMATH)ss.
CITY OF KLAMATH FALLS)

I, _____, Recorder (Deputy Recorder) for the City of Klamath Falls, Oregon, do hereby certify that the foregoing is a true and correct copy of a Resolution duly adopted by the Council of the City of Klamath Falls, Oregon, at the meeting held on the 20th day of October, 2008, and thereafter approved and signed by the Mayor and attested by the Deputy Recorder.

City Recorder (Deputy Recorder)

CITY OF KLAMATH FALLS
POLICY ON IDENTITY THEFT PREVENTION & RED FLAG ALERTS

Adopted **October 20, 2008**

Purpose of Policy

This policy has been developed to address the requirements of the Fair and Accurate Credit Transaction Act provisions of the federal Fair Credit Reporting Act Rule 16, CFR §681.2 (the FTC "Red Flag Rules") and the Oregon Consumer Identity Theft Protection Act ("OCITPA") set forth in ORS 646A.600, *et seq*. Under these laws, the City of Klamath Falls ("City") must take appropriate measures to guard personal, confidential information, Covered Accounts and Covered Account holders from identity fraud/theft. The purpose of this policy is to identify patterns, practices, or specific activities that indicate the possible existence of Identity Theft and to take all reasonable steps to prevent and mitigate the theft of personal information from Covered Accounts. Under the Red Flag Rules, the City must by November 1, 2008 adopt rules for identifying and detecting "Red Flags" that raise concerns that Covered Account information is potentially being misused or stolen, and, under OCITPA, the City must implement safeguards for protecting the security, confidentiality and integrity of personal information entrusted to the City by its customers and employees, including the proper disposal of such information.

Definitions

"Covered Accounts" are accounts used mostly for personal, family, or household purposes that involve multiple payments or transactions and may include deferred payments for services or property. Covered Accounts include utility accounts and any account where the extension of credit is offered resulting in a continuing relationship. Covered Accounts also include 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.

"Identity Theft" is a fraud committed or attempted using the "Identifying Information" or "Personal Information" of another person without authority.

"Identifying Information" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. Identifying Information includes a person's:

- 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
- Routing code

"Personal Information" includes a consumer or employee's name in combination with: a SSN; a passport or any federal ID number; an ODL or Oregon Identification card number; or a financial, credit, or debit card number along with a security code, access code or password. It may also include the same types of information without the name if the information obtained would be sufficient to permit a person to commit Identity Theft against the person whose information was compromised.

"Private Information" is a collective reference to Identifying Information and Personal Information.

"Red Flag" is any pattern, practice or specific activity that indicates the possible existence of Identity Theft. Alerts, notifications, or other warnings received from local law enforcement or other governmental organizations can be regarded as Red Flags for Identity Theft. Such information may include a fraud alert or the United States Post Office providing a notice of address discrepancy.

"Security Breach" means any unauthorized acquisition of computerized data, including hard copies, that materially compromises the security, confidentiality or integrity of Personal Information, but does not include any good faith acquisition or use of Personal Information for legitimate purposes, including law enforcement investigations. A Security Breach occurs when it is known that Private Information (excluding names, addresses and phone numbers): has been lost; is out of city staff's physical control; or has in any way been acquired without authorization.

Policy

- In compliance with the Red Flag Rules, the City shall implement a program taking all reasonable steps to detect, prevent, and mitigate instances of Identity Theft, the misuse of Identifying Information and opportunities for a Covered Account holder to misuse account information. To carry out this policy, the City has adopted and will implement the rules set forth in this Policy: to identify and detect Red Flags raising concerns that Identifying Information or Covered Account holder information is potentially being misused or stolen; and to outline procedures for safeguarding Private Information.
- In compliance with OCITPA, the City of Klamath Falls shall implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of Personal Information, including its proper disposal.
- This Policy includes five primary compliance areas: 1) determining what Private Information the City holds; 2) being aware of potential Red Flags; 3) safeguarding Personal Information entrusted to the City by its customers and employees; 4) providing notice of Security Breaches and the theft or misuse of Personal Information; and 5) implementing the Policy.

Identifying Information

The City collects a substantial amount of Private Information through a variety of processes which require staff to assess and address risks associated with the collection of Private Information and to make a good faith attempt to verify the identity of a person opening any account with the City Prospective applicants who wish to receive a specific service must submit a separate application or provide verbally, the following information:

- name of adult members on the account;
- address location where service shall be provided;
- Social Security number, driver's license number or Tax Identification Number;
- contact and billing information; and
- a valid government issued photo identification as proof of identity (sometimes).

Other types of Private Information commonly used or collected by the City include, but are not limited to, documents which contain sensitive data such as:

- Public Employee Retirement System (PERS) forms such as Designation of Beneficiary (SSN of employee);
- Release of PERS Information (SSN of employee);
- Employment application information (SSN of candidate, driver's license);
- Non-Employee Profile (SSN and ODL of candidate);
- Background Check Form (SSN and ODL of candidate);
- Employee Files [primarily HR (personnel and medical files)];
- License applications and related information (SSN of applicant, driver's license);
- Medical information (medical history, SSN of patient); or
- Housing loan criteria (SSN of applicant, income verification).

It is the City's responsibility to prevent and mitigate Identity Theft regarding any Private Information or Covered Account holder information. The City currently uses procedures, processes and tools to properly identify customers and employees prior to accessing or distributing account information. The City information systems employ various security tool sets to mitigate Identity Theft.

Red Flags

Categories of Red Flags associated with customer accounts or the ability to initiate a customer account may include:

- inquiries inconsistent with the history and usual pattern of activity of a customer including such things as a recent and significant increase in the volume of inquiries;
- an unusual number of recently established credit relationships;
- a material change in the use of services, or other unusual activity associated with the account;
- an account that was closed for cause or identified for abuse of account privileges;
- documents provided for identification that appear to have been altered or forged;
- the photograph or physical description on the presented identification is not consistent with the appearance of the applicant or customer presenting the identification;

- other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification;
- other information on the identification is not consistent with readily accessible information that is on file, such as a prior customer file; or
- an application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Categories of Red Flags may also include personal Identifying Information provided by a person that is inconsistent when compared against external information sources such as:

- an address that does not match any address in the HTE data file;
- a Social Security Number that does not match previous history for the same customer;
- personal Identifying Information provided by the customer that is not consistent with other personal Identifying Information provided by the customer;
- personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources;
- an address on an application is the same as the address provided on a fraudulent application;
- a phone number on an application is the same as the number provided on a fraudulent application;
- personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources;
- an address on an application is fictitious, a mail drop, or a prison;
- a phone number that is invalid, or is associated with a pager or answering service;
- a Social Security Number provided is the same as that submitted by other persons opening an account or other customer;
- an address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers;
- a person opening the account fails to provide all required personal Identifying Information on an application or in response to notification that the application is incomplete;
- personal Identifying Information provided is not consistent with information that is on file with the City; or
- the person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report in response to a challenge question.

Other unusual or suspicious activity indicating Red Flags may include:

- shortly following the notice of a change of address for a customer account, the City receives a request for the addition of authorized users on the account;
- mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account;
- the City is notified that the customer is not receiving their bill;
- the City is notified of unauthorized charges or transactions in connection with the customer's account;

- payments are made in a manner associated with fraud; or
- an existing account with a stable history shows irregularities.

Red Flag notifications and warnings from credit reporting agencies and other entities may include:

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on a customer or applicant;
- Notice or report from a credit agency of an active duty alert for an applicant;
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity; or
- 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.

Safeguarding Identifying Information

In the event a report indicates a Red Flag or an information discrepancy, it will be reported to the employee's supervisor for further review and verification of the information, including verifying identification in person at the City. Staff shall also report to their supervisor when it appears that account documents have been altered or forged when compared to other documents in a customer or employee file. It shall be brought to management's attention immediately if any customer, employee or applicant presents an invalid identification, or identification that appears forged for the purpose of obtaining access to account information.

Access to account information will be permitted in person at the City, only after verifying the person's identity through photo identification. Account information may also in the future be obtained over the internet with secure password protection. Access to customer account information via telephone or internet (when available) shall require the customer to verify his or her identity using information that would only be known to the customer as reflected in the customer's account. Staff will make note in a customer's file when there is a lack of correlation between information provided by a customer and information contained in a file for the purposes of gaining access to account information. Information will not be given without first clearing any discrepancies in the information provided.

For the protection of Social Security Numbers ("SSNs") the following activities are prohibited: Printing SSNs on any mailed materials not requested by the employee or customer unless redacted [meaning no more than the last four (4) digits is readable or accessible]; or Printing SSNs on cards used to access products, services, or City buildings (such as ID cards); or publicly posting or displaying SSNs. Exemptions to these prohibitions include: requirements by the state of Oregon; requirements of federal laws, such as W2s, W4s, 1099s, etc; records that are required by law to be made available to the public; records for use for internal verification or administrative processes; and records used for enforcing a judgment or court order.

Staff will no longer request sensitive data on certain forms if the data is not absolutely necessary. Documents will be purged and destroyed that have reached destruction schedule dates. Sensitive documents retained by the City will be stored in locking files or behind locked

doors. Any documents containing sensitive information will be destroyed or shredded prior to disposal.

Staff will note unusual use of accounts, or suspicious activities related to accounts and promptly notify management when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the customer or employee.

Staff will monitor transactions and verify the validity of change of address requests, in the case of existing accounts. Social Security Numbers or Tax Identification Numbers will not be provided by staff either verbally or in writing, even where a customer is asking for his/her own information.

If the City discovers that any of its customers or employees have become a victim of Identity Theft through personal information used by the organization in opening or maintaining an account, management shall take appropriate steps that it deems necessary to mitigate the impacts of such Identity Theft. These steps may include, but are not limited to:

- monitoring an account for evidence of Identity Theft;
- contacting the customer;
- changing any passwords, security codes, or other security devices that permit access to an account;
- reopening an account with a new account number;
- closing an existing or compromised account;
- not attempting to collect on an account;
- notifying law enforcement; and/or
- determining that no response is warranted under the particular circumstances.

Third Party Vendors

The City has various business relationships with third party contractors. Under these business relationships, the third party contractor may have access to customers' Private Information covered under this policy. The City shall ensure that the third party contractor's work for the organization is consistent with this policy by:

- Amending City contract templates to incorporate these requirements; or
- By determining through written acknowledgment that the third party contractor has reasonable alternative safeguards that provide the same or a greater level of protection for customer information as provided by the organization.

Notice of Theft

Notice from customers or employees, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with customer or employee accounts can potentially be a Red Flag for Identity Theft. Upon notice of Identity Theft, the City will contact the customer or employee directly in order to determine what steps may be necessary to protect any customer information in the possession of the City. Such steps may include, but are not limited to, setting up a new account for the customer or employee with additional Identifying Information that may be identified only by the customer or employee, in order to protect the integrity of the account.

Notification of Security Breach

In the event that Personal Information has been subject to a Security Breach, the Finance Director will provide notification of the breach to the customer(s) or the employee(s) as soon as possible in compliance with OCITPA. In general, this requires that the notification be provided in any of the following methods: in writing; electronically, if that is the primary manner of communication with the customer or employee; or by telephone if the affected person is contacted directly. The exception to the notification requirement is if the notification would impede a criminal investigation, and a law enforcement agency has requested in writing that the notification be delayed.

Implementation

The City Manager's Office is responsible for assuring that the implementation of this policy is carried out and for the creation of an Identity Theft Committee composed of management employees. The Identity Theft Committee will monitor Identity Theft issues and propose changes to this Policy to improve the City's efforts in protecting the security, confidentiality and integrity of personal information entrusted to the City by its customers and employees. The City Manager is authorized to amend this Policy as deemed appropriate.

The Human Resources Department is responsible to include this Identity Theft Prevention and Red Flag Alert Policy as part of new employee orientation by documenting review of this policy and the concepts in "Identity Theft – A Business Guide". The business guide is posted at: {Insert Address on City website}.

Department directors are responsible to be familiar with the Identity Theft Protection Act and to meet with their staff to assess current compliance and document appropriate safeguard practices in writing. Department directors are also responsible to include this policy in temporary employee orientation by documenting review of this policy and the concepts in "Identity Theft – A Business Guide."

Employees are responsible to comply with this policy and any internal processes as directed by their department. If a Security Breach occurs, the person discovering the breach (or that employee's supervisor) shall notify the Finance Director, who is responsible for notifying the person(s) whose information has been compromised in the manner required by OCITPA. Noncompliance may result in formal disciplinary action up to and including termination of employment. Employees should contact their supervisor if they have questions about compliance with this policy.

The Finance Department is responsible for developing a security check list to be used by each department to ensure proper procedures are followed. Upon review and adherence to the checklist, each department must confer with the Finance Department regarding any compliance issues or concerns.

Information Systems is responsible for establishing technical controls to safeguard Private Information stored in electronic format and for documenting those safeguard practices in writing.

Review and Update

This policy shall be reviewed annually in October by the Finance Department and updated as necessary.