

COUNCIL POLICY NO. C-13

TITLE: Identity Theft Prevention Program

POLICY: See attachment.

REFERENCE: Salem City Council Finance Committee Report dated November 7, 2011, Agenda Item No. 3 (a)
Supplants Administrative Services Report dated April 27, 2009, Agenda Item No. 4.2 (c)

City of Salem

Identity Theft Prevention Program

Effective May 1, 2009

I. PURPOSE

In 2003, the Federal Trade Commission adopted 16 C.F.R. § 681.2 (“Red Flag Rule”), which implements Section 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. According to the Red Flag Rule, municipalities are creditors subject to FACTA. In 2007, the State of Oregon enacted ORS 646A.622, the Oregon Consumer Identity Theft Protection Act, (OCITPA). Under these laws, every financial institution and creditor is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. The Identity Theft Prevention Program must contain reasonable policies and procedures to:

- A. Identify relevant patterns, practices, or specific activities (red flags) that may indicate the existence of identity theft related to new and existing covered accounts 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. Update periodically to reflect changes in risks to customers or to the safety and soundness of information to prevent identity theft.

The purpose of the City’s Identity Theft Prevention Program (the “Program”) is to comply with the Red Flag Rule and OCITPA by providing for the detection, prevention, and mitigation of identity theft in connection with the opening of a new covered account or with an existing covered account with the City, and providing for continued administration of the Program for compliance with changes to the Red Flag Rule and the OCITPA. The Program was developed with oversight by the Program Administrator. 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 is appropriate to the size, complexity and nature of the City’s operations, and approved the Program on April 20, 2009.

II. DEFINITIONS

- A. **Customer** means a person to whom the City provides services.
- B. **Covered Account** means:
 1. Any account the City offers to, or maintains for, customers that is primarily for personal, family or household purposes, and that involves multiple payments or transactions; and

2. Any other account that the City offers or maintains for persons where there is a reasonably foreseeable risk of identity theft.

C. **Identity Theft** means fraud committed using the personal information of another.

D. **Personal Information** means:

1. A customer's first name, or first initial and last name, in combination with one or more of the following:
 - a. The customer's social security number;
 - b. The customer's driver's license number or state identification card number issued by the Oregon Department of Transportation;
 - c. The customer's passport number or other identification number issued by the United States; or
 - d. The customer's financial account number, credit or debit card number, in combination with a security code, access code or password that would permit access to the customer's financial account.
2. The information in Section 1 is not "Personal Information" when the information is rendered inaccessible through encryption, redaction, or other security method, and the encryption key or other security method has not been acquired by an unauthorized person.
3. "Personal Information" does not include information in a federal, state or local government record that is lawfully made available to the public in compliance with Public Records Laws.

E. **Program Administrator** means the Director of Finance, or appointed designee.

F. **Red Flag** means a pattern, practice, or specific activity that indicates possible Identity Theft.

G. **Security Breach** means the unauthorized acquisition of Personal Information.

H. **Security Information** means government data, the disclosure of which would likely place the security of information, individuals, or property in substantial jeopardy of theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury.

III. IDENTITY THEFT PROTECTION.

- A. City departments, divisions, and employees shall only collect Personal Information for appropriate business reasons, including, but not limited to, the opening of an account, making a payment on an account, or the application of a license or permit. Examples

include, but are not limited to, City water or sewer utility accounts, program loans, library account information, or applications for permits.

- B. The City will safeguard Personal Information in its possession, unless disclosure is required by law.
- C. Personal Information shall not be printed on mailed materials unless the Personal Information has been redacted in such a way as to render the information unusable for identity theft. Personal Information shall not be printed on cards used to access products, services, or City buildings. Personal Information shall not be included on public postings or displays, including the City's web site. Personal Information may be used by City staff for internal verification or administrative purposes.
- D. The City will maintain reasonable safeguards for the custody and disposal of Personal Information so as to prevent disclosure. Each City Department shall establish administrative, technical, and physical safeguards to protect Personal Information maintained by the Department.
 - 1. Administrative safeguards shall include assigning an employee to coordinate a security program, to identify internal and external risks, and to train employees.
 - 2. Technical safeguards shall include assessing risks in network and software design; in information processing, transmission, and storage; and in testing and monitoring controls.
 - 3. Physical safeguards shall include locking material containing Personal Information in file cabinets or storage systems; electronic data kept on a secured server; detecting, preventing, and responding to intrusions that could result in the disclosure of Personal Information; and protecting Personal Information from unauthorized access.
- E. Each City Department is responsible for the proper disposal of Personal Information after the Personal Information is no longer needed for City business purposes. Proper disposal may include shredding or rendering the material unreadable by other means.
- F. Each City employee shall take the following actions to safeguard Personal Information, whether in paper or electronic form:
 - 1. Social security number shall not be collected or used unless there is an appropriate business reason, or the collection or use is required by law.
 - 2. Social security numbers shall not be printed on cards or documents that are mailed to customers or publicly displayed unless the customer has requested the information that requires a social security number. Examples include, by way of illustration, a copy of a credit application or employment application.
 - 3. Credit card receipts shall not include the full credit card number of the customer.
 - 4. Paper documents containing Personal Information shall be stored in locked cabinets and storage systems, or in locked rooms or locked storage areas.
 - 5. If an employee has computer access to Personal Information, the employee's computer shall be password protected and include an active password protected screen saver.

6. Observable confidential or individually identifiable information shall be shielded from unauthorized disclosure on computer screens and paper documents.

IV. RED FLAGS.

In addition to the procedures covered under the Program in Section III, each Department shall identify “Red Flags” that will allow detection of the misuse or theft of Personal Information. A Red Flag may be a pattern, practice, or specific activity that may indicate the existence of Identity Theft.

A. Identifying Red Flags

To identify Red Flags, each Department shall consider the types of accounts that it offers and maintains, the methods it provides to open accounts, the methods it provides to access the accounts, the methods applied to closing accounts, and any previous experiences with Identity Theft. The following shall be considered Red Flags by each Department:

1. Notifications and Warnings from Credit Reporting Agencies

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

2. Suspicious Documents

- a. Identification document or card that appears to be forged, altered, or inauthentic.
- b. Identification document or card on which a customer’s or applicant’s photograph or physical description is not consistent with the person presenting the document.
- c. Other document with information that is not consistent with existing customer information. Example: a person’s signature on a check appears forged.
- d. Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information

- a. Identifying information presented that is inconsistent with other information the customer provides. Example: inconsistent birth dates.

- b. Identifying information presented that is inconsistent with other sources of information. Example: an address not matching an address on a credit report.
- c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.
- d. Identifying information presented that is consistent with fraudulent activity. Example: an invalid phone number or fictitious billing address.
- e. Social security number presented that is the same as one given by another customer.
- f. An address or phone number presented that is the same as that of another person.
- g. A person fails to provide complete personal identifying information on an application when reminded to do so.
- h. A person's identifying information is not consistent with the information that is on file for the customer.

4. Suspicious Account Activity or Unusual Use of Account

- a. Change of address for an account followed by a request to change the account holder's name.
- b. Payments stop on an otherwise consistently up-to-date account.
- c. Account used in a way that is not consistent with prior use. Example: very high activity.
- d. Mail sent to the account holder is repeatedly returned as undeliverable.
- e. Notice to the City that a customer is not receiving mail sent by the City.
- f. Notice to the City that an account has unauthorized activity.
- g. Breach in the City's computer system security.
- h. Unauthorized access to or use of customer account information.

5. Alerts from Others

Notice to the City from a customer, identity theft victim, law enforcement or other person that a fraudulent account has been opened or maintained for a person engaged in identity theft.

B. Detecting Red Flags.

- 1. New Accounts.** In order to detect any of the Red Flags associated with opening a *new account*, City personnel shall take the following steps to obtain and verify the identity of the person opening the account:
 - a. Require multiple forms of 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;
 - b. Review documentation showing the existence of a business entity; and/or

c. Independently verify the information provided.

2. Existing Accounts. In order to detect any of the Red Flags identified above for an *existing account*, City personnel shall take the following steps to the extent possible to monitor transactions with an account:

- a. Verify the identification of customers if they request information, either in person, via telephone, via facsimile, via email;
- b. Verify the validity of requests to change billing addresses; and
- c. Verify changes in banking information given for payment purposes.

C. Preventing and Mitigating Identity Theft

In the event an employee detects a Red Flag, the employee shall immediately contact the Program Administrator and continue to monitor the account for evidence of identity theft. The Program Administrator shall investigate the matter and determine the appropriate response, which should include one or more of the following actions:

1. Notify the Customer.
2. Not open a new account.
3. Close an existing account.
4. Reopen an account with a new number.
5. Notify law enforcement.
6. Determine that no response is warranted under the particular circumstances.

If a Red Flag is detected, the Program Administrator shall determine whether a Security Breach has, or is likely to have, occurred and take appropriate action as outlined in Section V.

V. SECURITY BREACH.

If the Program Administrator determines a Security Breach has, or is likely to have, occurred, the following actions are required:

- A. The Program Administrator shall immediately report the security breach to the City Manager.
- B. The Program Administrator shall, as soon as possible, notify all persons whose Personal Information was subject to a security breach by one of the following methods:
 1. Written notification;
 2. Electronic notification, if this is the customary means of communication with the person;
 3. Telephone notice, provided that direct contact with the person is made; or
 4. Substitute notice as provided in ORS 646A.604.

- C. The notice provided to the customer shall include:
1. A description of the incident in general terms;
 2. The approximate date of the security breach;
 3. The type of Personal Information obtained as a result of the security breach;
 4. The contact information of the Program Administrator or the Program Administrator's designee in order for the customer to have direct contact for questions or concerns about the incident;
 5. Contact information for national customer reporting agencies; and
 6. Information to the customer to report suspected identity theft to law enforcement, including the Federal Trade Commission.

D. An incident response team designated by the Program Administrator shall investigate any security breach and provide a written report to the City Manager assessing the situation and actions to be undertaken, if necessary.

VI. PROGRAM UPDATES

- A. **Time for Updates.** The Program Administrator shall review the Program when changes in risks to customers or to the safety and soundness of the City's practices in reducing the risks of customers from Identify Theft occur.
- B. **Considerations when Updating.** In reviewing the Program, the Program Administrator shall consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention, and changes in the City's business arrangements with other entities.
- C. **Recommend Changes to Program.** 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 recommend changes to the City Manager who shall refer the Program updates to the City Council for proposed adoption.

VII. SERVICE PROVIDER CONTRACTS

If the City engages a service provider (the "Contractor") to perform an activity or service that involves processing, storing, or transmitting customer personal, financial, or account information, the contract shall include a clause that:

- A. "Contractor acknowledges that it is the City's responsibility to ensure that activities of all service providers and contractors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, and shall comply with the federal Fair and Accurate Credit Transactions Act of 2003, as amended, and the Oregon Consumer Identity Theft Protection Act (ORS 646A.600 to 646A.628), as amended. By contractor signature hereon, the contractor certifies and warrants that contractor maintains its own Identity Theft Prevention

- Program, consistent with the guidance of the red flag rules (16 C.F.R. Part 681) and validated by appropriate due diligence;
- B. Contractor agrees to defend, indemnify, and hold harmless the City, its officers, employees, and agents from and against any and all claims arising out of or related to Contractor violating: (i) the federal Fair and Accurate Credit Transactions Act of 2003, as amended; (ii) the Oregon Consumer Identity Theft Protection Act (ORS 646A.600 to 646A.628), as amended;
 - C. A statement that in the event of a breach of customer personal, financial, or account information, the contractor will immediately notify the City and take steps to reduce the risk of identity theft; and if applicable; and
 - D. A statement that vendor's software and data transmission process is, and will remain, compliant with Payment Card Industry (PCI) Data Security Standards (DSS)."

VIII. PROGRAM ADMINISTRATION.

A. Responsibility and Oversight.

Responsibility and oversight for developing, implementing and updating the Program lies with the Program Administrator. The Program Administrator shall appoint an Identity Theft Committee. At least one member of the Committee shall have detailed technical knowledge of the City's information technology systems.

B. Responsibility for Implementation.

The Program Administrator shall be responsible for the Program implementation and oversight of Department compliance, for ensuring Departments provide adequate training on the Program, for determining which steps of prevention and mitigation should be taken in particular circumstances, and for considering and recommending changes to the Program.

C. Internal Audits.

A compliance audit will be conducted annually on a component, department, or division covered by this program by the Administrative Services Finance Division Chief Accountant.

D. Staff Training and Reports.

The Program Administrator shall ensure that City staff responsible for the Program are trained. Training shall include the goals of the Program, how to protect Personal Information, how to detect Red Flags, and how to take steps responsive to a Red Flag. Department Heads are responsible for the Program compliance for their Departments, and shall periodically meet with their staff to assess current compliance and document appropriate safeguard practices. Department Heads responsible for the Program will provide reports to the Program Administrator on incidents of Identity Theft.

E. Non-disclosure of Specific Practices.

For the effectiveness of this Identity Theft Prevention Program, knowledge about Red Flag identification, detection, mitigation and prevention practices shall be limited to the Identity Theft Committee and employees who implement the Program.

Documents produced in order to develop or implement the Program shall be considered “security information” and unavailable to the public because public disclosure would substantially jeopardize the security of information against improper use and circumvent the City’s Identity Theft prevention efforts, thereby facilitating the commission of Identity Theft. Employees shall comply with the Program and any internal processes adopted by the City Manager, the Identity Theft Prevention Committee, and Department Heads. Noncompliance may result in formal disciplinary action, up to and including termination of employment. Employees should contact their immediate supervisor or Program Administrator if they have questions about compliance with the Program or any implementing measures.