

**CITY OF PEORIA, ARIZONA  
COUNCIL COMMUNICATIONS**

cc: 4C  
Amend No. \_\_\_\_\_

Date prepared: 04/01/09

Council Meeting Date: 04/21/09

**TO:** Carl Swenson, City Manager  
**FROM:** Brent Mattingly, Finance Director *Pone*  
**PREPARED BY:** Vicki Rios, Revenue Manager *VR*  
**SUBJECT:** Identity Theft Prevention Program

**RECOMMENDATION:**

That the Mayor and Council adopt Resolution 09-44 establishing a program and policies governing the identification, detection, and mitigation of identity theft; making the Chief Financial Officer responsible for the program; and providing for an effective date of May 1, 2009.

**BACKGROUND:**

As part of the Fair and Accurate Credit Transactions Act of 2003 16 C. F. R. § 681.2 "Rules", the Federal Trade Commission (FTC) issued regulations requiring creditors to adopt a program which provides for identification, detection, and response to patterns, practices, or specific activities known as Red Flags that could indicate identity theft. These Rules are generally known as the FTC "Red Flag Rules."

A municipal utility is considered a creditor and is subject to the Rules because it supplies utility services to customers who establish an account, use services, receive a bill, and pay for services after they are rendered. Therefore, all municipal utilities must develop and adopt an Identity Theft Prevention Program by May 1, 2009.

The Finance Department, Revenue Division ("Division") is responsible for establishing, maintaining, billing, collecting, and servicing of all of the City's utility accounts. Led by the Division, a team of staff from the Finance and Information Technology Departments worked together to assess the risk of identity theft on city utility accounts and developed the attached Identity Theft Prevention Program (Exhibit A). Highlights of the policy include:

1. Identification of the various Red Flags
2. Information about how to detect Red Flags

**CITY CLERK USE ONLY:**

- Consent Agenda  
 Carry Over to Date: \_\_\_\_\_  
 Approved  
 Unfinished Business (Date heard previous: \_\_\_\_\_)  
 New Business  
 Public Hearing: No Action Taken

ORD. # \_\_\_\_\_ RES. # 09-44  
LCON# \_\_\_\_\_ LIC. # \_\_\_\_\_  
Action Date: \_\_\_\_\_

3. Steps for staff members to follow when responding to Red Flags
4. Steps and processes used to protect our customer's personal information

The Division already has many policies and measures in place to prevent and detect identity theft. With the implementation of this program, utility customers may see some additional steps required to verify their identity before they gain access to their account. For example, a customer may need to show identification for an in-person transaction or they may be asked additional questions to verify their identity to complete transactions over the telephone. These added measures are designed to help protect our customers from identity theft.

The Identify Theft Prevention Program will be administered by a committee under the direction and oversight of a Program Administrator who will be the Chief Financial Officer or his/her designee. All employees responsible for implementing the program will be trained in preventing, detecting, and mitigating identity theft. The Program Administrator will report to the City Council each January regarding the effectiveness of the program and will recommend changes to the program as necessary.

Identity thieves use stolen personal information to open new accounts and misuse current accounts, causing harm to consumers and businesses. Therefore, staff recommends the City Council adopt the attached resolution approving the attached Identity Theft Prevention Program, making the Chief Financial Officer responsible for the program, and making the program effective May 1, 2009.

**ATTACHMENT:**

1. Resolution 09- 44

**RESOLUTION NO. 09-44**

**RESOLUTION OF THE MAYOR AND COUNCIL OF THE CITY OF PEORIA, MARICOPA COUNTY, ARIZONA, ADOPTING A PROGRAM AND POLICIES GOVERNING THE IDENTIFICATION, DETECTION AND MITIGATION OF IDENTITY THEFT, AND PROVIDING FOR AN EFFECTIVE DATE.**

WHEREAS, the Mayor and Council of the City of Peoria, Arizona (the "City"), have determined that it is in the public interest to provide a program to govern the overall prevention of identity theft.

WHEREAS, the Chief Financial Officer exercises the day to day authority over the management of the Identity Theft Prevention Program.

THEREFORE, it is resolved by the Mayor and Council of the City of Peoria, Maricopa County, Arizona as follows:

**SECTION 1. ADOPTION OF THE IDENTITY THEFT PREVENTION PROGRAM**

That the Mayor and Council adopt and approve the policies attached as Exhibit "A" as an official guideline for the prevention of identity theft.

**SECTION 2. RESPONSIBILITY OF THE CHIEF FINANCIAL OFFICER**

That the Chief Financial Officer is authorized and directed to manage the Identity Theft Prevention Program in accordance with these adopted guidelines and policies.

**SECTION 3. EFFECTIVE DATE**

That the Chief Financial Officer is authorized and directed to make the Identity Theft Prevention Program effective on May 1, 2009.

**ADOPTED AND APPROVED this 21<sup>st</sup> day of April, 2009.**

---

**Bob Barrett, Mayor, City of Peoria, Arizona**

ATTEST:

---

Mary Jo Kief, City Clerk, City of Peoria,  
Arizona

APPROVED AS TO FORM:

---

Stephen M. Kemp, City Attorney, City of  
Peoria, Arizona

ATTACHMENTS:

EXHIBIT A – Identity theft Prevention Program

EXHIBIT A

 <p><b>ADMINISTRATIVE PROCEDURE</b></p>	<p>AP _-_ <i>[assigned by CMO]</i> Category: <i>[One of pre-existing list]</i></p>
	<p>Department: <i>Finance</i></p>
<p><b>TITLE:</b> <i>Identity Theft Prevention Program</i></p>	<p>Approved: <i>[Date is 10 days following Council's review period. Date is entered by City Manager's Office Staff]</i></p>

A. Purpose

Identity thieves use stolen personal information to open new accounts and misuse current accounts, causing harm to consumers and businesses. The City of Peoria ("City") Finance Department, Revenue Division ("Division") developed this Identity Theft Prevention Program ("Program") as required by the Federal Trade Commission ("FTC") pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("Rules") 16 C. F. R. § 681.2. These Rules are generally known as FTC "Red Flag Rules." The Rules support the Program which provides for identification, detection, and response to pattern, practices, or specific activities known as Red Flags that could indicate Identity Theft. The Division is responsible for establishing, maintaining, billing, collecting, and servicing of all of the City's utility accounts and, according to the Rules, a municipal utility is a creditor subject to the Rules.

This Program was developed with oversight and approval of the City Council. After consideration of the size and complexity of the Division's operations and accounting systems, and the nature and scope of the Division's activities, the City Council determined that this Program was appropriate for the Division.

B. Definitions

The following terms shall have the following meanings:

1. "City" shall mean the City of Peoria
2. "Division" shall mean the Revenue Division of the City Finance Department

3. **"Program" shall mean the Identity Theft Prevention Program contained herein.**
4. **"Red Flag Rules" or "Rules" shall be policies adopted in compliance with the requirements established by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions Act of 2003 16 C. F. R. § 681.2. These Rules are generally known as FTC "Red Flag Rules."**
5. **"Red Flag" shall mean a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.**
6. **"Identity Theft" shall mean "fraud committed or attempted using the identifying information of another person"**
7. **"Identifying information" shall mean "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 (IP) address, or routing code.**
8. **"Creditors" shall mean "An entity that regularly extends, renews, or continues credit; any entity that regularly arranges for extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Any person or entity that provides a product or service for which the consumer pays after delivery is also a creditor.**
9. **"Covered account" shall mean:**
  - a. **An account a creditor offers or maintains for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, auto loans, cell phone accounts, utility accounts, and bank accounts.**
  - b. **Any other account offered or maintained for which there is a reasonably foreseeable risk to customers, or to the safety and soundness of the creditor, from Identity Theft.**

**C. Policy Requirements**

Utility service accounts held by customers, whether residential, commercial or industrial, are covered by the Rules. Under the Rules, every creditor is required to establish a Program tailored to its size, complexity and the nature of its operations. Each program must contain reasonable policies and procedures for:

**1. Identification of Red Flags**

In order to identify relevant Red Flags, the Division has taken into consideration 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 Division has identified the following Red Flags, in each of the listed categories:

**a. Notifications and Warnings From Credit Reporting Agencies**

- 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; and
- 4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

**b. Suspicious Documents**

- 1) Identification documents or credit cards that appears to be forged, altered or inauthentic;
- 2) Identification documents or credit cards on which a person's photograph or physical description is not consistent with the person presenting the document;
- 3) Other documents 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**

- 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

- 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 Utility that a customer is not receiving mail sent by the Utility;
- 6) Notice to the Utility that an account has unauthorized activity;
- 7) Breach in the Utility's computer system security; and
- 8) Unauthorized access to or use of customer account information.

e. Alerts from Others

- 1) Notice to the Utility 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.

2. Detection of Red Flags

a. New Accounts

- 1) In order to detect any of the Red Flags identified above associated with the opening of a new account, Division personnel will take the following steps to obtain and verify the identity of the person opening the account:

- a) Require certain identifying information such as name, residential or business address, principal place of business for an entity, driver's license or other identification;
  - b) Verify the customer's identity (for instance, review a driver's license or other appropriate forms of identification);
  - c) Review documentation showing the existence of a business entity or independently contact the customer.
- b. Existing Accounts
- 1) In order to detect any of the Red Flags identified above for an existing account, Division personnel will take the following steps to monitor transactions with an account:
    - a) Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
    - b) Verify the identity of customers requesting changes in billing addresses; and
    - c) Verify the identity of customers changing banking or other information given for billing and payment purposes.
- c. Responding to Red Flags
- 1) In the event Division personnel detect any identified Red Flags, such personnel will respond by taking one or more of the following steps, depending on the degree of risk posed by the Red Flag:
    - a) Contact the customer;
    - b) Continue to monitor an account for evidence of Identity Theft;
    - c) Change any passwords or other security devices that permit access to accounts;
    - d) Not open a new account;
    - e) Close an existing account;
    - f) Reopen an account with a new number;
    - g) Notify the Program Administrator for determination of the appropriate step(s) to take;
    - h) Notify law enforcement; or
    - i) Determine that no response is warranted under the particular circumstances.

3. Protecting Customers Information

- a. In order to further prevent the likelihood of Identity Theft occurring with respect to the covered accounts, the Division will take the following steps with respect to its internal operating procedures to protect customer identifying information:
- 1) Require and keep only the kinds of customer information that are necessary for business purposes;
  - 2) Ensure that its website is secure or provide clear notice that the website is not secure;
  - 3) Ensure complete and secure destruction of paper documents and computer files containing customer information per the City's established record retention policies;
  - 4) Ensure that office computers are password protected and that computer screens lock after a set period of time;
  - 5) Secure offices and workspaces containing customer information;
  - 6) Ensure computer virus protection is up to date.
- b. In the event the Division engages a service provider to perform an activity in connection with one or more accounts, the Division 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 Division's Program and report any Red Flags to the Program Administrator.

4. Management Oversight

- a. Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee. The chairman of the committee will be the Program Administrator who may be the Chief Financial Officer or his or her appointee. The committee consists of two or more other individuals appointed by Program Administrator. At least one committee member will be from the City's Information Technology Department. The Program Administrator will be responsible for ensuring all required City staff are trained on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps taken to prevent and mitigate Identity Theft, for determining which steps of prevention and mitigation should be taken in particular circumstances and for considering periodic changes to the Program.

5. Staff Training

- a. Division 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. Training will occur:
  - 1) At the inception of the Program, general training will be conducted for all staff with access to the utility account information.
  - 2) Subsequent training will occur any time the Program is amended or once a year, whichever comes first.

#### 6. Reporting

- a. All staff is required to report any incident of Identity Theft to the Program Administrator.
- b. The Program Administrator shall compile all incidents of Identity Theft and recommend necessary changes to the Identity Theft Committee for their approval.
- c. The Program Administrator will report to the City Council in January of each year regarding any material matters and issues regarding the program including items such as:
  - 1) The initial implementation;
  - 2) Employee training;
  - 3) Effectiveness of policies and procedures in addressing the risk of Identity Theft;
  - 4) Service provider (third party) arrangements;
  - 5) Recommendations for changes.

#### 7. Program Updates

- a. This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Division from Identity Theft. At least once a year, the Program Administrator will consider the Division's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Division maintains and changes in the Division's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator 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.

#### 8. Program Elements and Confidentiality

- a. For the effectiveness of Identity Theft prevention Programs, the Red Flag Rules envision a degree of confidentiality regarding the Division's specific practices relating to Identity Theft detection, prevention and

mitigation. Therefore, under this Program, knowledge of such specific practices is limited to the Identity Theft Committee 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.

APPROVED:

Bob Barrett, Mayor

APPROVED AS TO FORM:

Stephen M. Kemp, City Attorney

APPROVED:

4/21/09, Resolution #09-44