

RESOLUTION 10-05

A RESOLUTION OF THE MAYOR AND COUNCIL OF THE CITY OF HOLBROOK, ARIZONA, ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

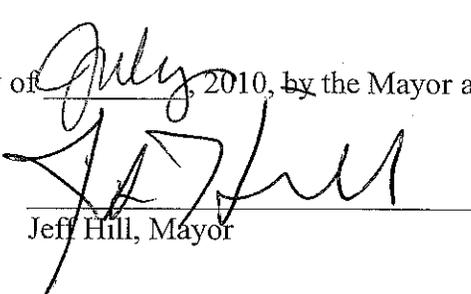
WHEREAS, the Fair and Accurate Credit Transaction Act of 2003, an amendment to the Fair Credit Reporting Act, required rules regarding identity theft protection to be promulgated; and

WHEREAS, the rules became effective November 1, 2008, and required municipal utilities and other departments to implement an identity theft prevention program and policy by December 31, 2010, the enforcement date; and

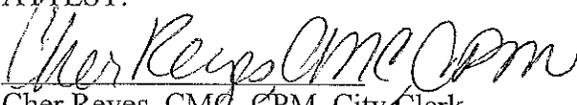
WHEREAS, The City of Holbrook has determined that the following policy is in the best interest of the municipality and its citizens.

NOW, THEREFORE, BE IT RESOLVED by the Mayor and Council of the City of Holbrook, Arizona, that the attached identity theft prevention program is hereby approved.

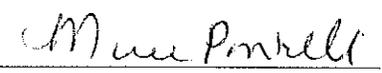
PASSED AND ADOPTED this 13<sup>th</sup> day of July, 2010, by the Mayor and Council of the City of Holbrook, Arizona.

  
\_\_\_\_\_  
Jeff Hill, Mayor

ATTEST:

  
\_\_\_\_\_  
Cher Reyes, CMC, CPM, City Clerk

APPROVED AS TO FORM:

  
\_\_\_\_\_  
Marlene Pontrelli, City Attorney

# Fraud Policy of the City of Holbrook

## **Background:**

To combat the growing problem of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and charged the Federal Trade Commission (FTC) with publicizing rules regarding identity theft (the “Red Flags Rule”). The City of Holbrook recognizes the importance of protecting its citizens against fraud and has developed this policy to increase controls that will aid in the detection and prevention of fraud. This policy is also intended to provide all stakeholders both internal and external with the knowledge that allegations of impropriety will be investigated objectively, fairly, and promptly.

## **Scope:**

Management is responsible for the detection and prevention of fraud, misappropriations, and other inappropriate conduct. Fraud is defined as an intentional deception, misappropriation of resources or the manipulation of data to the unfair or unlawful advantage or disadvantage of a person or entity. This policy is designed to fulfill the requirements of the Red Flags Rule. To comply this policy must:

1. Identify the Red Flags for identity theft the City is likely to come across.
2. Set up procedures to detect those Red Flags in day-to-day operations.
3. Respond appropriately to prevent and mitigate the harm done.
4. Keep the program current and educate City staff.

## **A. Identifying Red Flags**

### **1. Suspicious Documents**

- Identification that looks altered or forged
- The person presenting the identification does not look like the photo or match the physical description
- Information on the identification that differs from what the person presenting the identification is telling you or does not match with other information, like a signature card or recent check
- An application that looks like it has been altered, forged, or torn up and reassembled

### **2. Suspicious Personal Identifying Information**

- Any inconsistencies with what else you know
- Any inconsistencies in the information the customer has given you

- An address, phone number, or other personal information that has been used on an account you know to be fraudulent
- A false or bogus address, an address for a mail drop or prison, a phone number that is invalid, or one that is associated with a pager or answering service
- A Social Security number that has been used by someone else opening an account
- An address or telephone number that has been used by many other people opening accounts
- A person who omits required information on an application and does not respond to notices that the application is incomplete
- A person who cannot provide authenticating information beyond what is generally available from a wallet or credit report

### **3. Suspicious Account Activity**

- A new account that is used in ways associated with fraud – for example, the customer does not make the first payment, or makes only an initial payment
- An account that is used in a way inconsistent with established patterns
- An account that has been inactive for a long time is suddenly used again
- Mail sent to the customer that is returned repeatedly as undeliverable although transactions continue to be conducted on the account
- Information that the customer is not receiving their account statements in the mail
- Information about unauthorized charges on the account

### **4. Notice from Other Sources**

- A notice from a customer, a victim of identity theft, a law enforcement authority, or someone else

## **B. Detecting Red Flags**

### **1. New Accounts**

- 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
- Verify the customers identity for example review a drivers license or other documentation
- Review documentation showing the existence of a business entity
- Independently contact the customer

## **2. Existing Accounts**

- Verify the identification of customers if they request information
- Monitor transactions
- Verify the validity of requests to change billings addresses
- Verify changes in banking information given for billing and payment purposes

## **C. Prevent and Mitigate Identity Theft**

### **1. Actions after Detecting**

- Monitor the covered account for evidence of identity theft
- Contact the customer
- Close an existing account
- Reopen an account with a new account number
- Not opening a new account
- Not trying to collect on an account or not selling an account to a debt collector
- Notifying law enforcement
- Determining that no response is warranted under the particular circumstances

The facts of a particular case may warrant using one or several of these options, or another response altogether.

#### **D. Update the Policy**

The City recognizes that new red flags emerge as technology changes or identity thieves evolve their tactics. This policy will be periodically reviewed for updates to ensure that it keeps current with identity theft risks. At least once a year the City will factor in experiences with fraud and address any changes that maybe identified in the policy.

#### **E. Administering the Policy**

The responsibility for developing, implementing and updating this policy lies with the City Manager. The City Manager will be responsible for ensuring staff is trained regarding the detection of Red Flags and the steps for preventing and mitigating identity theft. Training will only be required as necessary. Trained staff may not need to be retrained if they have already received anti-fraud training.

The City Manager should report annually to the Council. The report will evaluate how effective the program has been, identify significant incidents and responses, and recommend changes to the program.

The City currently contracts with certain service providers whose activities are covered by the rule. The City ensures that the activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The City will supply the service providers a copy of this policy and any reports about red flags that they have detected.