Identity Theft Prevention Program

CITY OF CODY
WYOMING

Revised 11/12

Introduction

In compliance with the Fair Credit Reporting Act all utility companies are required to develop and implement an Identity Theft Prevention Program. The program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and protecting sensitive information. The rule was issued by the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

This program is intended to identify red flags that will (1) alert City employees when accounts are opened using false information; (2) protect against the establishment of false accounts: (3) develop methods to ensure existing accounts were not opened using false information; (4) to protect sensitive information contained in existing accounts; and (5) develop measures to respond to fraudulent activity.

The steps required to develop an Identity Theft Prevention Program are:

- Assess existing identity theft risk (risk assessment) for new and existing accounts.
- Use the risk assessment to select measures (red flags) that may be used to detect attempts to establish fraudulent accounts.
- Identify procedures for employees to prevent the establishment of false accounts and procedures for employees to implement if existing accounts are being manipulated.
- Obtain program approval by the City Council.
- Train the appropriate employees on the program's policies and procedures.
- Update the plan annually with review and approval by the City Council.

Scope

All utility companies are required to comply with this rule even if only nominal information such as name, phone number and address are collected. Since the City of Cody collects customer information for a variety of purposes not related to utilities other City departments have been evaluated and included in this program.

Sensitive Information

Sensitive information includes the following, whether stored in electronic or printed format:

- Credit Card Information – credit card number, expiration date, cardholder name, cardholder address
- Bank Account Information – bank account number, account holder name, account holder address
- Tax Identification Numbers – social security number and federal employer ID number

- Other Personal Information – name, date of birth, mailing and physical address, driver's license number, government ID number, phone number and medical information

Detection (red flags)

The City of Cody adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary. City staff will use the following criteria to determine if the potential for fraud or identity theft exists on new and existing accounts:

Alerts & Notifications

- Alerts, notifications, or other warnings received from customers or law enforcement regarding possible identity theft.

- Identity theft is discovered by City employees

Suspicious Documents & Information

- Documents provided for identification appear to be forged or altered

- The photograph or physical description on the identification is not consistent with the appearance of the person providing the information

- Other information on the identification is not consistent with the information provided by the person associated with the account.

- Customer fails to provide all information requested

Suspicious Activity Related to the Account

- Request for frequent mailing address changes.

- Request to add, remove or change the name on the account and requestor cannot or will not provide adequate verification of identity

- Mail sent to the address on file is returned repeatedly as undeliverable although transactions continue to occur on the account.

Suspicious Personal Indentifying Information

- Personal information provided by applicant does not match other sources of information on file.

- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)

- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- Social security number or driver's license number is the same as that of another customer

- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet

Response

Upon detecting a red flag the City must take specific actions to mitigate the threat. Any employee that may suspect fraud or detect a red flag will take the following actions, as applicable:

- Gather all related documentation and prepare a summary of the situation.
- Provide initial research to the Director of Administrative Services, or his/her designee.
- The Director of Administrative Services or his/her designee shall determine the merits of the potential red flag.
- If the situation is determined to be fraudulent, the appropriate action shall be taken which may include but is not limited to:
    a. Cancelling the account
    b. Notifying and cooperating with legal counsel and law enforcement
    c. Determining the extent of the liability to the City of Cody
    d. Notifying the actual customer that fraud has been attempted

In determining an appropriate response, the City should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records. Such incidents may require additional action.

Sensitive Information Security Procedures

The City of Cody adopts the following security procedures for all functions which are identified as high-risk functions:

<u>New Accounts</u>

- Obtain identifying information about and verifying the identity of the person opening the account
    a. Copy of valid driver's license or U.S. Government issued photo ID
    b. For accounts where the account holder is a corporation or LLC a company photo ID and/or letter of authorization on company letterhead authorizing the signer of the application to open the account is permitted in lieu of a driver's license or U.S. Government issued photo ID

<u>Existing Accounts</u>

- Authenticating customer identity prior to providing account information
    a. Use of account passwords or verification of personal data listed on the account (SSN, EIN, or driver's license number)

- Authenticating customer identity prior to changing personal information such as name, mailing address and phone number
    a. Use of account passwords or verification of personal data listed on the account (SSN, EIN, or driver's license number)

Access to Customer Records

- Paper documents, files, and electronic media containing sensitive information will be stored in a secure file room or locked filing cabinets. Storage rooms containing documents with sensitive information and record retention areas shall be locked after business hours or when unsupervised. After-hours access is restricted to specifically identified employees. Access to areas in which sensitive information is stored is restricted to authorized City employees only.

- Files containing sensitive information shall be kept in the secure file room or locked filing cabinet except when an employee is working on the file.

- Desks, workstations, work areas, printers, fax machines and common work areas will be cleared of all documents containing sensitive information when not in use.

- Employees will log out of computer programs containing sensitive information when they will be away from their work areas for more than 5 minutes.

- Visitors who must enter areas where sensitive information is kept must be escorted by an employee of the City.

- Background checks will be done before hiring employees who will have access to sensitive information.

- Access to sensitive information is limited to employees with a "need to know."

- Paper records containing sensitive information will be shredded before being placed into the trash.

- Electronic storage devices shall be purged and overwritten according to IT policy prior to disposal.

- Sensitive information shall not be stored on laptops unless the information is encrypted or password protected.

- Computer passwords will be required for all employees using programs containing sensitive information.

- Passwords will not be shared or posted near workstations.

- Passwords will be changed periodically.

Periodic Updates to the Program

An annual review will be performed each November to determine whether all aspects of this program are up to date and applicable to the current business environment. This review will include:

- An assessment of the sensitive information covered under this program
- A review of red flags, which may be revised, replaced or eliminated
- A review of actions to take in the event fraudulent activity is discovered
- A review of staff training status and content

Reporting Requirements

A report will be prepared annually and submitted to the City Council. This report shall include a summary of the oversight and effectiveness of the program, a summary of any identity theft incidents and the response to the incidents, and recommendations for substantial changes to the program, if any.

Staff Training

Staff training shall be conducted for all employees that have access to or come into contact with sensitive information. Employees shall receive annual training in all elements of this program and to ensure maximum effectiveness employees shall receive additional training as changes to the program are made. All new employees that will have access to or come into contact with sensitive information shall receive training on this policy within 1 month of their hire date. The employee's supervisor and the employee shall both sign an acknowledgement of training form which shall be submitted to Administrative Services.

Program Administration

This program is the responsibility of the City Council to implement and adopt annually. The operational responsibility of the program is delegated to the Administrative Services Director or his/her designee.