Red Flag Policy and Identity Theft Prevention Program

(as amended January 15, 2019, Resolution 2019-02)

Purpose

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Definitions

1. **Covered Account** means:

    a. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

    b. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2. **Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

3. **Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.

4. **Customer** means a person that has a covered account with a creditor

5. **Identity theft** means a fraud committed or attempted using identifying information of another person without authority.

6. **Notice of address discrepancy** means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. **§** 1681(c)(h)(l), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

7. **Person** means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

8. **Personal Identifying Information** means a person's credit card account information, debit card information, bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.

9. Red flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

10. **Service provider** means a person that provides a service directly to the City.

11. **City** means the City of Fruita.

Findings

1. The City is a creditor pursuant to 16 CFR **§** 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.

2. Covered accounts offered to customers for the provision of City services include utility accounts and development review accounts.

3. The process of opening a new covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur.

4. The City limits access to personal identifying information to those employees responsible for or otherwise involved in opening covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered directly into the City's computer system and is not otherwise recorded.

5. The City determines that there is a low risk of identity theft occurring in the following ways:

a. Use by an applicant of another person's personal identifying information to establish a new covered account; and

b. Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts.

Access to Covered Account Information

1. Access to customer accounts shall be password protected and shall be limited to authorized City personnel.

2. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the City Clerk and the password changed immediately.

3. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the City Clerk.

Credit Card Payments

1. In the event that credit card payments that are made over the telephone are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.

2. All documentation containing personal identifying information shall be shredded erased, or otherwise modified to make the personal identifying information unreadable or indecipherable through any means after credit card payment has been entered into computer database.

3. Account statements and receipts for covered accounts shall include only the authorization code issued after approval of the credit card transaction from the third party service provider for payment of the covered account.

Sources and Types of Red Flags

All employees responsible for or involved in the process of opening a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

1. Alerts from consumer reporting agencies, fraud detection agencies or service providers.

Examples of alerts include but are not limited to:

a. A fraud or active duty alert that is included with a consumer report;

b. A notice of credit freeze in response to a request for a consumer report;

c. A notice of address discrepancy provided by a consumer reporting agency;

d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

i. A recent and significant increase in the volume of inquiries;
ii. An unusual number of recently established credit relationships;
iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. Suspicious documents. Examples of suspicious documents include:

a. Documents provided for identification that appear to be altered or forged;
b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;

c. Identification on which the information is inconsistent with information provided by the applicant or customer;

d. Identification on which the information is inconsistent with readily accessible information that is on file with the creditor, such as the application for service; or

e. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

3. Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:

a. Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:

i. The address does not match any address in the consumer report; or

ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.

c. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the financial institution or creditor.

d. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.

e. The SSN provided is the same as that submitted by other applicants or customers.

f. The 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 applicants or customers.

g. The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

h. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.

i. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activity include:

a. Shortly following the notice of a change of address for an account, City receives a request for the addition of authorized users on the account.

b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

c. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

i. Nonpayment when there is no history of late or missed payments;
ii. A material change in purchasing or spending patterns;

d. An account that has been inactive for a long period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

f. The City is notified that the customer is not receiving paper account statements.

g. The City is notified of unauthorized charges or transactions in connection with a customer's account.

h. The City is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

5. Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

Prevention and Mitigation of Identity Theft

1. In the event that any City employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the City Clerk. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the City Clerk, who may in his or her discretion determine that no further action is necessary. If

the City Clerk in his or her discretion determines that further action is necessary, a City employee shall 1) notify the customer within thirty (30) days after the date of the determination that a security breached occurred 2) provide a copy of such notification to the Colorado Attorney General's office and 3) perform one or more of the following responses, as determined to be appropriate by the City Clerk:

a. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:

i. change any account numbers, passwords, security codes, or other security devices that permit access to an account; or

ii. close the account;

b. Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;

c. Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or

d. Take other appropriate action to prevent or mitigate identity theft.

2. In the event that any City employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect to an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the City Clerk. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the City Clerk, who may in his or her discretion determine that no further action is necessary. If the City Clerk in his or her discretion determines that further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate by the City Clerk:

a. Request additional identifying information from the applicant;

b. Deny the application for the new account;

c. Notify law enforcement of possible identity theft; or

d. Take other appropriate action to prevent or mitigate identity theft.

Updating the Program

The City Council shall annually review and, as deemed necessary by the Council, update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in

risks to customers or to the safety and soundness of the City and its covered accounts from identity theft. In so doing, the City Council shall consider the following factors and exercise its discretion in amending the program:

1. The City's experiences with identity theft;

2. Updates in methods of identity theft;

3. Updates in customary methods used to detect, prevent, and mitigate identity theft;

4. Updates in the types of accounts that the City offers or maintains; and

5. Updates in service provider arrangements.

Program Administration

The City Clerk is responsible for oversight of the program and for program implementation. The City Manager is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the City Manager, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program shall be submitted to the City Council for consideration by the Council.

1. The City Clerk will report to the City Manager at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:

> a. The effectiveness of the policies and procedures of City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
>
> b. Service provider arrangements;
>
> c. Significant incidents involving identity theft and management's response; and
>
> d. Recommendations for material changes to the Program.

2. The City Clerk is responsible for providing training to all employees responsible for or involved in opening a new covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The City Clerk shall exercise his or her discretion in determining the amount and substance of training necessary.

Outside Service Providers

In the event that the City engages a service provider to perform an activity in connection with one or more covered accounts the City Clerk shall exercise his or her discretion in reviewing such

arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.

Treatment of Address Discrepancies

Pursuant to 16 CFR § 681.1, this establishes a process by which the City will be able to form a reasonable belief that a consumer report relates to the consumer about whom it has requested a consumer credit report when the City has received a notice of address discrepancy. In the event that the City receives a notice of address discrepancy, the City employee responsible for verifying consumer addresses for the purpose of providing the municipal service or account sought by the consumer shall perform one or more of the following activities, as determined to be appropriate by such employee:

1. Compare the information in the consumer report with:

    a. Information the City obtains and uses to verify a consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 3 1 U.S.C. *§* 53 18(1);

    b. Information the City maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or

    c. Information the City obtains from third-party sources that are deemed reliable by the relevant City employee; or

2. Verify the information in the consumer report with the consumer.

Furnishing Consumer's Address to Consumer Reporting Agency

1. In the event that the City reasonably confirms that an address provided by a consumer to the City is accurate, the City is required to provide such address to the consumer reporting agency from which the City received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:

    a. The City is able to form a reasonable belief that the consumer report relates to the consumer about whom the City requested the report;

    b. The City establishes a continuing relation with the consumer; and

    c. The City regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.

2. Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the City to such agency for the reporting period in which the City establishes a relationship with the customer.

Methods of Confirming Consumer Addresses

The City employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

1. Verifying the address with the consumer;

2. Reviewing the City's records to verify the consumer's address;

3. Verifying the address through third party sources; or

4. Using other reasonable processes.

Destruction of Personal Identifying Information

Unless otherwise required by state or federal law or regulation, when paper and electronic documents containing personal identifying information are no longer needed, employees of the City must destroy or arrange for the destruction of such documents by shredding, erasing, or otherwise modifying the personal identifying information in the documents to make the personal identifying information unreadable or indecipherable through any means.

Where the destruction of records is performed by a third party service provider, the City shall ensure that the provider maintain reasonable security procedures and practices that are appropriate for the records subject to destruction and are reasonably designed to protect the records from unauthorized access, use, modification, disclosure, or destruction.

For the purposes of this section "personal identifying information" means: a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, (as defined below); an employer, student, or military identification number; or a financial transaction devise, (as defined below).

For the purposes of this section "biometric data" means: unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

For the purposes of this section "financial transaction devise" means: any instrument or device whether known as a credit card, banking card, debit card, electronic fund transfer card, or guaranteed check card, or account number representing a financial account or affecting the financial interest, standing, or obligation of or to the account holder, that can be used to obtain cash, goods, proper, or services or to make financial payments. Financial transaction devise does not mean a "check", a "negotiable order of withdrawal", or a "share draft".

Questions concerning appropriate means for disposing of specific types of paper or electronic documents should be directed to the City Clerk.