# CHAPTER 34
# PRIVACY CONCERNS: IDENTITY THEFT



## ARTICLE I. Identity Theft Identification Program

Sec. 34-1-1. Short Title. This article shall be known as the Identity Theft Prevention Program.

Sec. 34-1-2. Purpose. The purpose of this Article is to comply with 16 CFR § 681.2, as may be amended from time to time in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

Sec. 34-1-3. Definitions. For purposes of this Article, the following definitions apply:

(a) "City" means the City of Searcy, Arkansas.

(b) "Covered account" means (i) 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 (ii) 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 identify theft, including financial, operational, compliance, reputation, or litigation risks.

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

(d) "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.

(e) "Customer" means a person that has a covered account with a creditor.

(f) "Identify theft" means a fraud committed or attempted using identifying information of another person without authority.

(g) "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(h) "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.

(i) "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(j) "Service provider" means a person that provides a service directly to the City.

Sec. 34-1-4. 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 sanitation service fees, building and inspection permits and related fees, and business and occupation license fees.

(3) The city has not had previous experience with identity theft related to covered accounts but is required by the Federal Trade Commission to adopt ordinances of this nature.

(4) The processes of opening a new covered account, restoring an existing covered account, and making payments on such accounts, have been identified by the Federal Trade Commission as potential processes in which identity theft could occur.

(5) The City limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring 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.

(6) There is a 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;

b. Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name;

c. 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; and

d. Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account, or other method of payment.

Sec. 34-1-5. Process of Establishing a Covered Account.

Sec. 34-1-5.1 As a precondition to opening a covered account in the City, each applicant shall provide the City with personal identifying information of the customer: (1) a valid government issued identification card containing a photograph of the customer or, for customers who are not natural persona, a photograph of the customer's agent opening the account; or (2) if deemed necessary by the department, "Such applicant shall also provide any information necessary providing the service for which the covered account is created to access the applicant's consumer credit report." Such information shall be entered directly into the City's computer system and shall not otherwise be recorded.

Sec. 34-1-5.2 Each account shall be assigned an account number and personal identification number (PIN) which shall be unique to that account. The City may, but shall not be required so to do, utilize computer software to randomly generate assigned PINs and to encrypt account numbers and PINs.

Sec. 34-1-6. Access to Covered Account Information.

Sec. 34-1-6.1 Access to customer accounts shall be password protected and shall be limited to authorized City personnel.

Sec. 34-1-6.2 Such password(s) shall be changed by the director of the department providing the service for which the covered account is created, or if department director is not available, by the director of information technology, or department director designee on a regular basis, shall be at least 8 characters in length and shall contain letters, numbers and symbols.

Sec. 34-1-6.3 Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Mayor and Department Head and the password changed immediately.

Sec. 34-1-6.4 Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Mayor and Department Head and the City Attorney.

Sec. 34-1-7. Credit Card Payments.

Sec. 34-1-7.1 In the event that credit card payments that are made over the Internet are proceed 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.

Sec. 34-1-7.2 All credit card payments made over the telephone or the City's website shall be entered directly into the customer's account information in the computer data base.

Sec. 34-1-7.3 Account statements and receipts for covered accounts shall include only the last four digits of the credit or debit card or the bank account used for payment of the covered account.

Sec. 34-1-8. Sources and Types of Red Flags. All employees responsible for or involved in the process of opening a covered account, restoring 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) In the event the City elects to utilize consumer reporting agencies, alerts from those 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 for 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 financial institution or creditor, such as a signature card or a recent check; 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 of 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 identify theft or phishing relating to covered accounts.

Sec. 34-1-9. Prevention and Mitigation of Identify Theft.

Sec. 34-1-9.1 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 identify 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 Mayor, Department Head and City Attorney or appropriate legal counsel. 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 Mayor, and the Department Head, who may in his or her discretion determine that no further action is necessary. If the Mayor 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 City Attorney or appropriate legal counsel:

a. Contact the customer;

b. 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;

c. 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;

d. Notify a debt collector within a reasonable time and to use best efforts to do so within 24 hours of the discovery of likely or probably identity theft relating to a customer account that has been sold to such debt collector in the event that a customer's account has been sold to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;

e. 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

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

Sec. 34-1-9.2 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 reg flags to the Mayor or the Department Head. If, in his or her discretion, such employee deems that identity theft if unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Department Head, who may in his or her discretion determine that no further action is necessary. If the Department Head 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 Department Head:

a. Request additional identifying information from the applicant;

b. Deny the application for the new account;

c. Notify law enforcement of possible identify theft; or

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

Sec. 34-1-10. 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.

Sec. 34-1-11. Program Administration. The City Clerk-Treasurer is responsible for oversight of the program and for program implementation. The Mayor 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 Mayor, 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.

Sec. 34-1-11.1 The City Clerk-Treasurer will report to the Mayor 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.

Sec. 34-1-11.2 The City Clerk-Treasurer is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing 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-Treasurer shall exercise his or her discretion in determining the amount and substance of training necessary.

Sec. 34-1-12. 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-Treasurer 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 or 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. *(Ord. No. 2009-8, §1 4-14-2009)*