

RESOLUTION NO. 2008-206

A RESOLUTION OF THE LODI CITY COUNCIL  
APPROVING POLICIES AND PROCEDURES FOR  
CUSTOMER CREDIT SECURITY PROGRAM IN  
ACCORDANCE WITH THE FAIR & ACCURATE CREDIT  
TRANSACTIONS ACT OF 2003

=====

WHEREAS, the Fair & Accurate Credit Transactions ("FACT") Act of 2003 was enacted by Congress to curtail the effects of identity theft; and

WHEREAS, the FACT Act was recently amended to require all creditors (including local governmental agencies that defer payments for goods or services) to implement an identity theft prevention program by establishing policies and procedures utilizing warning signs, so called "red flags," as indicators of identity theft; and

WHEREAS, in accordance with the FACT Act, creditors must determine whether covered accounts are subject to a risk of identity theft, and, if necessary, implement a consumer credit protection program designed to detect, prevent, and mitigate identity theft in customer accounts. The program also should incorporate the creditor's existing policies and procedures where applicable and provide for continued administration of consumer credit protections. The Act requires that such a program be approved and implemented by November 1, 2008; and

WHEREAS, in order to meet the mandates of the FACT Act, City staff performed a needs assessment taking into account the existing business practices, policies, and procedures currently in place to safeguard customer identity, account information, and financial transactions associated with customers' utilities accounts and when appropriate modified or enhanced these policies and procedures to incorporate the four basic elements for detecting, preventing, and mitigating identity theft by enabling City's Financial Services Division to:

- (i) identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those "red flags" into the program;
- (ii) detect "red flags" that have been incorporated into the identity theft prevention program;
- (iii) respond appropriately to any "red flags" that are detected to prevent and mitigate identity theft; and
- (iv) ensure the identity theft prevention program is updated periodically to reflect changes in risks from identity theft; and

WHEREAS, to ensure compliance under the FACT Act, federal government regulators will be required to evaluate public agencies and their adherence to their identity theft prevention programs and when necessary impose fines where the disregard of "red flags" has resulted in losses to consumers.

WHEREAS, staff recommends approval of the *Policies and Procedures for Customer Credit Security Program in Accordance with the Fair & Accurate Credit Transactions Act of 2003* attached marked Exhibit A; and

WHEREAS, as indicated in the proposed *Policies and Procedures*, a subcommittee has been created to develop, implement, and administer the proposed program and will create, at least annually, a report on its compliance with the FACT Act for consideration by the Council. In addition, the Subcommittee will identify necessary changes, which, when implemented, will increase data security, automate manual processing, establish electronic audit trails by tracking history for all activities, and improve reporting capability, all of which serve to protect the credit information of City's utility customers.

NOW, THEREFORE, BE IT RESOLVED, that the Lodi City Council does hereby approve the *Policies and Procedures for Customer Credit Security Program in accordance with the FACT Act of 2003* as shown on Exhibit A attached hereto.

Dated: October 15, 2008

---

I hereby certify that Resolution No. 2008-206 was passed and adopted by the City Council of the City of Lodi in a regular meeting held October 15, 2008, by the following vote:

AYES: COUNCIL MEMBERS – Hansen, Hitchcock, Johnson, Katzakian,  
and Mayor Mounce

NOES: COUNCIL MEMBERS – None

ABSENT: COUNCIL MEMBERS – None

ABSTAIN: COUNCIL MEMBERS – None



RANDI JOHL  
City Clerk



**CITY OF LODI**

**PROCEDURES FOR CUSTOMER CREDIT SECURITY PROGRAM**

**PREPARED IN ACCORDANCE WITH THE  
FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003**

Approved by Resolution of the City Council on October 15, 2008  
Resolution No. 2008-\_\_\_\_\_

# PROCEDURES FOR CUSTOMER CREDIT SECURITY PROGRAM

## PREPARED IN ACCORDANCE WITH THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

### **Purpose.**

The purpose of this Program is to comply with 16 CFR § 681.2 (Fair & Accurate Credit Transaction Act of 2003) 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 for customers of the City of Lodi.

### **Definitions.**

For purposes of this Program, the following definitions apply:

- (a) 'City' means the City of Lodi.
- (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 identity 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 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.
- (9) 'Identity 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.
- (i) 'Privacy Officer' means that City employee designated by City's Deputy City Manager/Internal Services Director to administer City's Customer Credit Security Program under the direction of City's Financial Services Manager. The Privacy Officer will also oversee a committee of designated City employees charged with reviewing and recommending modifications and updates to the Program.
- (j) 'Red flag' means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- (k) 'Service provider' means a person that provides a service directly to the city.

### **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 electric, water, wastewater, refuse and other related charges/fees.
- (3) The processes of opening a new covered account, restoring an existing covered account, making payments on such accounts, and transferring services have been identified as potential processes in which identity theft could occur.
- (4) 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.
- (5) 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;
- 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;
- 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.

### **Process of Establishing a Covered Account.**

As a precondition to opening a covered account for City services, each applicant shall provide one form of the following personal identifying information:

- a. State issued Driver's License or Identification card;
- b. United States Passport;
- c. United States Military Identification; or
- d. United States Resident Alien Identification.

Each applicant shall also provide information necessary for the department providing the service for which the covered account is created to verify identity through a credit reporting agency.

Each applicant shall also provide written documentation of ownership or rental/lease agreement signed under penalty of perjury by both the applicant and the managing agent of the property.

Such information shall be entered directly into City's computer system and shall not otherwise be recorded.

### **Access to Covered Account Information.**

- (1) Access to customer accounts 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 Privacy Officer or in his/her absence the Financial Services Manager or designee.
- (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 Privacy Officer or in his/her absence the Financial Services Manager or designee.

### **Credit Card Payments.**

(1) In the event that credit card payments that are made over the Internet 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) 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.

### **Sources and Types of Red Flags.**

All City 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) 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 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.
- 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. 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 payment patterns;
- c. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
- d. City is notified that the customer is not receiving paper account statements.
- e. City is notified of unauthorized charges or transactions in connection with a customer's account.
- f. 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 Privacy Officer or in his/her absence the Financial Services Manager or designee. If, in his/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 Privacy Officer, who may in his/her discretion determine that no further action is necessary. If the Privacy Officer or in his/her absence the Financial Services Manager or designee determines that further action is necessary, a city employee shall perform one or more of the following responses, as determined to be appropriate:
- 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 two business days of the discovery of likely or probable 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.
- (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 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 Privacy Officer or in his/her absence the Financial Services Manager or designee. If, in his/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 Privacy Officer, who may in his/her discretion determine that no further action is necessary. If the Privacy Officer or in his/her absence the Financial Services Manager or designee in his/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:
- 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 this Program.**

The City Council shall annually review and, as deemed necessary, update this Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of 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 this Program:

- (1) 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 Privacy Officer under the direction of the Financial Services Manager is responsible for oversight of this Program and for Program implementation and is responsible for reviewing reports prepared by City staff regarding compliance with red flag requirements and with recommending material changes to the Program, as necessary in the opinion of the City Manager or City Attorney 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 and approval.

- (I) Privacy Officer in coordination with the Financial Services Manager will report to the City Manager and City Attorney at least annually, on compliance with the red flag requirements. The report will address material matters related to this 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 Privacy Officer or designee 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 this Program. The Privacy Officer in coordination with the Financial Services

Manager shall exercise their discretion in determining the amount and substance of training necessary.

**Outside Service Providers.**

In the event that City engages a service provider to perform an activity in connection with one or more covered accounts the Privacy Officer in coordination with the Financial Services Manager shall exercise their discretion in reviewing such arrangements in order to ensure, to the best of their 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.