

RESOLUTION NO. \_\_\_\_

RESOLUTION OF THE CITY OF MILPITAS  
ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Federal Trade Commission (“FTC”) has adopted regulations that require “creditors” holding consumer or other covered accounts which are used primarily for family, personal, or household purposes and involve or are designed for multiple payments or transactions to develop and implement by November 1, 2008, identity theft prevention programs that comply with those regulations; and

WHEREAS, because the City of Milpitas (“City”) provides utility services to its customers through an invoice payment account system and maintains other accounts, it is a “creditor” under the applicable FTC regulations and must therefore comply with those regulations by adopting and implementing an identity theft prevention program; and

WHEREAS, the City Council of the City of Milpitas desires to take action to comply with the applicable FTC regulations by adopting an identity theft prevention program that meets or exceeds all federal requirements and formalizes existing City practices.

NOW, THEREFORE, BE IT RESOLVED that the City Council hereby adopts and directs City staff to implement the attached Identity Theft Prevention Program.

PASSED AND ADOPTED this \_\_\_\_\_ day of \_\_\_\_\_ 2008, by the following vote:

AYES:

NOES:

ABSENT:

ABSTAIN:

ATTEST:

APPROVED:

\_\_\_\_\_  
Mary Lavelle, City Clerk

\_\_\_\_\_  
Jose S. Esteves, Mayor

APPROVED AS TO FORM:

\_\_\_\_\_  
Michael J. Ogaz, City Attorney

**CITY OF MILPITAS**

**IDENTITY THEFT PREVENTION PROGRAM**

**In Accordance with the  
Fair and Accurate Credit Transactions Act of 2003**

# INTRODUCTION

Regulations adopted by the Federal Trade Commission (“FTC”) pursuant to the Fair and Accurate Credit Transaction Act (“FACTA”) require public agencies such as the City of Milpitas (“City”) that act as creditors for purposes of such legislation to evaluate and formally adopt programs to detect, prevent, and mitigate identity theft before November 1, 2008. The City has a long history of protecting the personal financial and private information of its residents, businesses, and ratepayers. The following Identity Theft Prevention Program (“Program”) is intended to memorialize and outline the identity protections and procedures of the City and to formalize their continued use and update, as required by law.

To summarize, FACTA regulations require creditors like the City to adopt programs that can spot identity theft “red flags” (patterns, practices, or specific activities that indicate possible misuse or theft of personal financial information) and then act appropriately. In accordance with Federal Trade Commission guidelines and regulations, the City’s Program is broken up into four parts<sup>1</sup> and provides “reasonable policies and procedures” to do the following:

- 1) Identify “red flags” applicable to the types of financial or service accounts maintained by the City and incorporate those “red flags” into the Program;
- 2) Detect those “red flags” that have been incorporated into the Program as they occur;
- 3) Ensure that City staff respond appropriately to detected “red flags” so as to prevent and mitigate identity theft;
- 4) Ensure that the Program itself is updated periodically, to reflect changes in identity theft risk to City customers or the City;

The City places the highest priority on protecting any confidential financial and personal information submitted to it in the course of providing City services. The Program listed herein satisfies all FACTA requirements.

## **Section 1. Program “Red Flags”**

FACTA covers certain City transactions in which the City defers payment for goods or services. Most, if not all, such City transactions are those connected with the City collection of payments for the delivery of City utilities, such as for potable and recycled water and wastewater.

---

<sup>1</sup> Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003. 72 Fed. Reg. 63717, 63773 (Nov. 9, 2007) (codified at 16 CFR Part 681).

Under the FTC regulations, the City must identify those red flags that are relevant and applicable to its FACTA-covered activities. The following are those red flags that the City's Program is designed to spot:

- A. A consumer credit reporting agency reports the following in response to a credit check request:
  - 1) Fraud or active duty
  - 2) Credit freeze
  - 3) The Social Security Number (SSN) is invalid or belongs to a deceased person.
  - 4) The age or gender on the credit report is clearly inconsistent with information provided by the customers.
  
- B. Suspicious Documents
  - 1) Documents provided for identification appear to have been altered or forged.
  - 2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
  - 3) Other information on the identification is not consistent with information provided by customer.
  
- C. Suspicious Personal Identifying Information
  - 1) The SSN provided by the customer belongs to another customer in the Utility Billing system.
  - 2) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
  
- D. Unusual Use of, or Suspicious Activity Related to, the Covered Account
  - 1) A customer other than the account holder or co-applicant requests information or asks to make changes to an established utility account.
  - 2) A customer notifies the City of the following activities:
    - a) Utility statements are not being received
    - b) Unauthorized changes to a utility account
    - c) Fraudulent activity on the customer's bank account or credit card that is used to pay utility charges
  
- E. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor
  - 1) The City is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

## Section 2. Red Flag Detection

In connection with the opening and servicing of utility accounts, City Staff will take the following steps to detect the red flags identified in Section 1.

### A. New Accounts:

- 1) Require certain identifying information such as name, date of birth, SSN, residential or business address, telephone number, email address, driver's license or other identification; and
- 2) Verify the customer's identify (for instance, review a driver's license or other identification card); or
- 3) Review the Business License system to determine the existence of the business entity before establishing the utility account; or
- 4) Request a consumer credit report check

### B. Existing Accounts:

- 1) Verify the identification of customers using date of birth, SSN, telephone number, or email address if they request account information other than the outstanding balance owed; and
- 2) Verify the validity of requests to change billing addresses; and
- 3) Verify changes in banking information given for billing and payment purposes

## Section 3. City Response to Detected Red Flags

Each situation shall be evaluated on a case by case basis. Responses may include, but are not limited to, the following:

- 1) Marking an account in the Utility Billing system and monitoring it for evidence of identity theft;
- 2) Contacting the customer;
- 3) Not opening the new account;
- 4) Closing an existing account
- ~~5) Reopening an utility account with a new account number;~~
- ~~6) Notifying the appropriate law enforcement and/or prosecutorial agencies;~~  
~~and~~
- ~~7) Taking nNo action at all, if no identity theft or other malfeasance is found to have takenwas attempted or took place~~

## Section 4. Oversight of Program Administration

~~Under~~As required by FACTA regulations, ~~at the n identity theft prevention p~~Program shall ~~must~~ be overseen by ~~a the Ccity Ccouncil~~, an appropriate committee of the ~~Ccity cCouncil~~, or a designated employee at the level of senior management. ~~In the City's~~Under the Program, the Finance Director shall have the specific responsibility for the Program's implementation and to approve reports prepared by City Staff regarding compliance of the Program with FACTA regulations. Material changes to the Program as

necessary to address changing identity theft risks shall be reviewed by the Finance Director and approved by the City Manager.

By December 31 of every year, City Staff shall prepare a report on the City's compliance with FACTA regulations to the City Manager. The report shall address materials related to the Program and evaluate such issues as:

1. The effectiveness of the City's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
2. Security of service provider arrangements, if applicable;
3. Significant incidents involving identity theft and City management's response; and
4. Recommendations for material changes to the Program, if necessary.

Finally, whenever the City engages a service provider to perform an activity in connection with one or more covered accounts, the City shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. In this regard, the City may, if it deems appropriate, require the service provider to have policies and procedures to detect relevant red flags, as set forth in this Program.