
CITY OF ALTAMONT
ALTAMONT, ILLINOIS

ORDINANCE NO. 445-09
AN ORDINANCE ADOPTING
IDENTITY THEFT PREVENTION PROGRAM

ADOPTED BY THE
CITY COUNCIL
OF THE
CITY OF ALTAMONT

THIS 09th DAY OF MARCH 2009

PUBLISHED IN PAMPHLET FORM BY AUTHORITY OF THE CITY COUNCIL OF THE CITY OF ALTAMONT, EFFINGHAM COUNTY, ILLINOIS, THIS 09TH DAY OF MARCH 2009.

ORDINANCE 445-08

ORDINANCE OF THE CITY OF ALTAMONT, ILLINOIS
ADOPTING IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the federal Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which was signed into law on December 4, 2003, required the Federal Trade Commission and a number of federal banking agencies to issue joint rules and guidelines regarding the detection, prevention, and mitigation of identity theft by financial institutions and other creditors; and

WHEREAS, the Federal Trade Commission issued its final rules and guidelines implementing the pertinent portions of the FACT Act in late 2007 with an effective date of January 1, 2008 and a mandatory compliance date of May 1, 2009; and

WHEREAS, the FTC rules require utilities and all other creditors to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account, and the rules require the Program to include reasonable policies and procedures designed to accomplish the following:

- Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the utility from identity theft.

WHEREAS, the City of Altamont is subject to the FTC rules referenced above because it owns and operates municipal utilities for the provision of electric, water, waste water and sanitation services and bills its customers in arrears for such services; and

WHEREAS, the City Council of the City of Altamont, having considered its existing practices and past experiences regarding the opening of or access to utility accounts in light of the requirements of the FTC rules, has determined that the Identity Theft Prevention Program that is attached hereto and incorporated herein by this reference is appropriate and should be adopted and approved.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF ALTAMONT, EFFINGHAM COUNTY, ILLINOIS, AS FOLLOWS:

Section 1: The findings and determinations set forth in the preamble to this Ordinance are hereby made findings and determinations of the City Council of the City of Altamont and incorporated into the text of this Ordinance by this reference.

Section 2. The Identity Theft Prevention Program attached to this Ordinance is hereby adopted and approved by the City Council of the City of Altamont, Effingham County, Illinois.

Section 3. The Identity Theft Prevention Program shall be implemented and administered by the City Clerk as the Program Administrator.

Section 4. Changes to the Identity Theft Prevention Program of a day-to-day operational character and decisions relating to the interpretation and implementation of the Program may be made by the Program Administrator, however, major changes or shifts of policy positions under the Program shall only be made by the City Council.

Section 5. This Ordinance shall be in full force and effect from and after its passage.

PASSED, APPROVED AND ADOPTED by the City Council of the City of Altamont, Effingham County, Illinois, as required by law and approved by the Mayor this 09th day of March 2009.

LARRY E. TAYLOR, MAYOR

ATTEST:

SARAH STEPHEN, CITY CLERK

(MUNICIPAL SEAL)

STATE OF ILLINOIS)
 :
COUNTY OF EFFINGHAM)

I, Sarah Stephen, City Clerk of the City of Altamont, Effingham County, Illinois, do hereby certify that the foregoing pages constitute a true and correct copy of an Ordinance entitled "An Ordinance Adopting Identity Theft Prevention Program", and numbered 445-09, which was passed by the Council of the City of Altamont on March 09, 2009.

IN WITNESS WHEREOF, I have hereunto subscribed my name and affixed the corporate seal of said City of Altamont, all on this 09th day of March, A.D. 2009.

City Clerk

(SEAL)

STATE OF ILLINOIS)
 : SS
COUNTY OF EFFINGHAM)

CERTIFICATE

I, Sarah Stephen, certify that I am the duly appointed and acting Municipal Clerk for the City of Altamont, Effingham County, Illinois.

I further certify that on March 09, 2009, the Corporate Authorities of such municipality passed and approved Ordinance No. 445-09 entitled "An Ordinance Adopting Identity Theft Prevention Program" which provided by its terms that it should be published in pamphlet form.

The pamphlet form of Ordinance No.445-09, including the Ordinance and a cover sheet thereof was prepared, and a copy of such Ordinance was posted in the municipal building, commencing on March 09, 2009, and continuing for at least ten days thereafter. Copies of such ordinance were also available for public inspection upon request in the office of the Municipal Clerk.

Dated at Altamont, Illinois, this 19th day of March 2009.

Sarah Stephen, Municipal Clerk

(SEAL)

IDENTITY THEFT PREVENTION PROGRAM

City of Altamont, Illinois

This WRITTEN IDENTITY THEFT PROGRAM (the "Program") of the City of Altamont, Illinois is adopted as of Ordinance 445-09 by the Altamont City Council, pursuant to and in compliance with the Identity Theft Rules of the Federal Trade Commission (FTC), Part 681 of Title 16 of the Code of Federal Regulations (16 CFR Part 681).

Section 1. Purpose

The purpose of this Identity Theft Prevention Program is to protect customers of the Municipality's utility services from identity theft. The Program is intended to establish reasonable policies and procedures to facilitate the detection, prevention and mitigation of identity theft in connection with the opening of new Covered Accounts and activity on existing Covered Accounts.

Section 2. Scope

This Program applies to the creation, modification and access to Identifying Information of a customer of one or more of the utilities operated by the Municipality (electric, water, waste water, and sanitation) by any and all personnel of the Municipality, including management personnel. This Program does not replace or repeal any previously existing policies or programs addressing some or all of the activities that are the subject of this Program, but rather it is intended to supplement any such existing policies and programs.

Section 3. Definitions

When used in this Program, the following terms have the meanings set forth opposite their name, unless the context clearly requires that the term be given a different meaning:

Covered Account: The term "covered account" means an account that the Municipality offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments of transactions. (16 CFR 681.2(b)(3)(i)). A utility account is a "covered account." The term "covered account" also includes other accounts offered or maintained by the Municipality for which there is a reasonably foreseeable risk to customers the Municipality or its customers from identity theft. (16 CFR 681.2(b)(3)(ii)).

Identity Theft: The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority. (16 CFR §681.2(b)(8) and 16 CFR §603.2(a)).

Identifying Information: The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,

including any name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. Additional examples of "identifying information" are set forth in 16 CFR §603.2(a).

Red Flag: The term "Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Certain terms used but not otherwise defined herein shall have the meanings given to them in the FTC's Identity Theft Rules (16 CFR Part 681) or the Fair Credit Reporting Act of 1970 (15 U.S.C. §1681 *et seq.*), as amended by the Fair and Accurate Credit Transactions Act of 2003 into law on December 4, 2003. (Public Law 108-159).

Section 4. Administration of the Program

- (1.) Adoption and Changes. The initial adoption and approval of the Identity Theft Prevention Program shall be by Ordinance of the City Council. Thereafter, changes to the Program of a day-to-day operational character and decisions relating to the interpretation and implementation of the Program may be made by the City Clerk (Program Administrator). Major changes or shifts of policy positions under the program shall only be made by the City Council.
- (2.) Oversight. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of employees on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary recommending changes to the Program.
- (3.) Staff Training and Reports. Employees responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Each employee responsible for implementing the Program shall sign an Identity Theft Program Acknowledgement (attached hereto as Exhibit 1). Such training and acknowledgement will be sufficient to effectively implement the Program.
- (4.) Violation. The Program Administrator will be responsible for notifying the appropriate individual of any failure of the employees in adhering to the provisions of the Program. All employees have been advised that violations of the policies set forth herein may be grounds for disciplinary action or dismissal.
- (5.) Service Provider Arrangements Accounts. The Municipality will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

- (a) Require by contract, that service providers have such policies and procedures in place; and
- (b) Require, by contract service providers review the Utility's Program and report any Red Flags to the Program Administrator.

Section 5. Identity Theft Prevention Elements

(1) Identification of Relevant Red Flags The Municipality has considered the guidelines and the illustrative examples of possible Red Flags from the FTC's Identity Theft Rules and has reviewed the Municipality's past history with instances of identity theft, if any. The municipality hereby determines that the following are the relevant Red Flags for purposes of this Program given the relative size of the Municipality and the limited nature and scope of the services that the Municipality provides to its citizens:

(2) Suspicious Documents.

- (a) Documents provided for identification appear to have been altered or forged.
- (b) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- (c) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- (d) Other information on the identification is not consistent with readily accessible information that is on file with the Municipality, such as a signature card or a recent check.
- (e) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

(3) Suspicious Identifying Information.

- (a) Personal identifying information provided is inconsistent when compared against external information sources used by the Municipality.
- (b) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- (c) A customer's identifying information is the same as shown on other applications found to be fraudulent.
- (d) A customer's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).
- (e) The SSN provided is the same as that submitted by other persons opening an account or other 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 other persons opening accounts or other customers.
- (g) A customer fails to provide complete personal identifying information on an application when reminded to do so.

- (h) Personal identifying information provided is not consistent with personal identifying information that is on file with the Municipality.

(4) Unusual Use of, or Suspicious Activity Related to a Covered Account.

- (a) Shortly following the notice of a change of address for a covered account, the Municipality receives a request for the addition of authorized users on the account.
- (b) A new utility account is used in a manner consistent fraud patterns. For example: the customer fails to make the first payment or makes an initial payment but no subsequent payments.
- (c) A covered account with a stable history shows irregularities.
- (d) A covered account that has been inactive for a reasonably lengthy 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 usage of utility products or services continues in connection with the customer's covered account.
- (f) The Municipality is notified that the customer is not receiving paper account statements.
- (g) The Municipality is notified of unauthorized usage of utility products or services in connection with a customer's covered account.
- (h) The Municipality's computer system is breached.
- (i) Unauthorized access to or use of customer Account information.

(5.) Notice of Possible Identity Theft.

The Municipality received notice from a customer, a victim of identity theft, law enforcement authority or any other person regarding possible identity theft in connection with a Covered Account.

Section 6. Detection of Red Flags

- (1.) In order to detect any of the Red Flags identified above with the opening of a new Account, employees of the Municipality will take the following steps to obtain and verify the identity of the person opening the Account.
 - (a) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, SSN, drivers license or other identification.
 - (b) Verifying the customer's identity, copying, and reviewing a drivers license and one other identification card.
 - (c) Reviewing documentation showing the existence of a business entity
 - (d) Independently contacting the customer.

- (2.) In order to detect any of the Red Flags identified above for an existing Covered Account, municipal employees will take the following steps to monitor transactions with a Covered Account.
 - (a) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email)
 - (b) Verify the validity of requests to change billing addresses
 - (c) Verify change in banking information given for billing and payment purposes.

Section 7. Response to Detected Red Flags

If the responsible employees of the Municipality as set forth in the previous section are unable, after making a good faith effort, to form a reasonable belief that they know the true identity of a customer attempting to open a new account or modify or otherwise access an existing account based on the information and documentation provided by the customer and any third-party service provider, the Municipality shall not open the new account or modify or otherwise provide access to the existing account as the case may be. Discrimination in respect to the opening of new accounts or the modification or access to existing accounts will not be tolerated by employees of the Municipality and shall be grounds for immediate dismissal.

- (1.) In the event Municipal employees detect any identified Red Flags, such employee shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag
 - a. Monitoring a Covered Account for evidence of Identity Theft.
 - b. Contacting the customer.
 - c. Changing any passwords, security codes, or other security devices that permit access to Covered Account.
 - d. Reopening a Covered Account with a new account number.
 - e. Not opening a new Covered Account.
 - f. Closing an existing Covered Account.
 - g. Notifying law enforcement.
 - h. Determining that no response is warranted under the particular circumstances.
 - i. Notify the Program Administrator for determination of the appropriate step(s) to take.

Section 8. Prevention of Identity Theft

- (1.) In order to further prevent the likelihood of identity theft occurring with respect to Utility Accounts, the Municipality will take the following steps with respect to its internal operating procedures.
 - (a) Ensure complete and secure destruction of paper documents and computer files containing customer information, including documentation of such destruction.
 - (b) Ensure that office computers are password protected and that computer screens lock after a set period of time.
 - (c) Require only the last four digits of SSNs on customer applications.
 - (d) Limit access to Accounts to only employees that require access.

- (e) Ensure that computer screens are only visible to the employee accessing the Account.
- (f) Require customers to authenticate addresses and personal information, rather than Account representatives asking if the information is correct.

Section 9. Program Updates – Risk Assessment

This Program will be periodically reviewed and updated to reflect changes in risks to customer and the soundness of the Municipality from Identity Theft. At least once per year, the Program Administrator will consider the Municipality's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of Accounts the Municipality maintains and changes in the Municipality's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the City Council with recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

Exhibit 1

Identity Theft Program Acknowledgement

I hereby state and acknowledge that I have received a copy of the Identity Theft Program adopted by the Altamont City Council, that I am responsible for reviewing, understanding and complying with this Program, and that I understand that any violation of the City of Altamont identity theft procedures may result in disciplinary action up to and including dismissal.

Signature

Date

Print Name

WITNESSED:

PROGRAM ADMINISTRATOR

Signature

Date

Print Name