M E M O R A N D U M

TO: Mayor Prussing and Council Members

FROM: City Comptroller

RE: Resolution Adopting an Identity Theft Prevention Policy

DATE: May 25, 2009

The Fair and Accurate Credit Transactions Act of 2003 and regulations issued by the Federal Trade Commission (called Red Flag Rules) to implement this act, requires the City of Urbana to develop and implement a written identity theft prevention program.

Under these regulations, the City is required to identify and detect certain relevant warning signs or "Red Flags" of identity theft and describe appropriate responses that would prevent and mitigate identity theft. The plan must also be periodically updated and include a process to train city employees and supervise any service providers.

As a part of the Identity Theft Prevention Program, I have included a Personal Information Protection Policy which establishes certain operating policies and procedures to protect against the inadvertent disclosure of protected personal information.

RESOLUTION NO. 2009-06-022R

A RESOLUTION ADOPTING IDENTITY THEFT PREVENTION PROGRAM

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF URBANA, ILLINOIS, as follows:

WHEREAS, the United States Congress has enacted the Fair and Accurate Credit Transactions Act of 2003 which requires that creditors are required to develop written policies and procedures regarding the detection, prevention and mitigation of identity theft.

NOW, therefore be it resolved that the Identity Theft Prevention Program and the Personal Information Protection Policy attached hereto is hereby adopted.

PASSED by the City Council this _____ day of _____, 2009.

_____
Phyllis D. Clark, City Clerk

APPROVED by the Mayor this _____ day of _____, 2009

_____
Laurel Lunt Prussing, Mayor

IDENTITY THEFT PREVENTION PROGRAM

PURPOSE

The purpose of this Identity Theft Prevention Program is to protect customers of the City of Urbana from identity theft and 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.

The City has developed this program to comply with the Federal Trade Commission's Red Flag Rules, implemented under Section 114 of the Fair and Accurate Credit Transactions Act of 2003, pursuant to Part 681 of Title 16 of the Code of Federal Regulations (16 CFR Part 681).

DEFINITIONS

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Covered Accounts:

1. An account that the City of Urbana offers or maintains primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

2. Any other account that the City of Urbana offers or maintains for which there is a reasonably foreseeable risk to customers of identity theft.

Red Flag: Any pattern, practice or specific activity that indicates the possible existence of identity theft.

Identifying Information: 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 numbers, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification numbers.

PROGRAM ADMINISTRATION

The initial adoption and approval of the Identity Theft Prevention Program shall be by the Mayor and 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 Comptroller who shall be the Program Administrator.

At least once a year, the Program Administrator will address the following issues:

1. The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of new covered accounts and activity with existing covered accounts.
2. Service provider arrangements
3. Significant incidents involving identity theft and management's response
4. Recommendations for material changes to the program, if needed, for improvement.

COVERED ACCOUNTS

The City performed an initial risk assessment to determine whether the City offers or maintains any accounts for which there are reasonably foreseeable risks to customers or the City from identity theft. In making this determination, the City considered 1) the methods it uses to open accounts 2) the methods it uses to access its accounts, and 3) its previous experience with identity theft, and has determined the following areas are "covered accounts":

1. Landscape Recycling Center charge accounts
2. Residential/Multi Family Recycling Tax program
3. Rental Registration program
4. A Service Provider Arrangement whereby the Urbana-Champaign Sanitary District administers the City's Sewer Benefit Tax
5. Community Development loan and grant programs
6. All Financial accounts which permit payments for personal services or similar transactions
7. Use of a consumer credit report from a consumer reporting agency for employment or credit purposes.

IDENTITY THEFT PREVENTION ELEMENTS

Identification of Relevant Red Flags

The City has considered the guidelines of possible Red Flags from the FTC's Identity Theft Rules. The following are relevant Red Flags for purposes of this program given the relative size of the City and the nature of the services provided to its citizens:

1. Suspicious documents:
   - Documents provided for identification appear to have been altered or forged.
   - An application that appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

2. Suspicious Personal Identifying Information:
   - Personal identifying information provided is inconsistent when compared against external sources.
   - Personal identifying information is the same type associated with fraudulent activity (ex. fictitious address, mail box drop or prison; or phone number is invalid or associated with a pager or answering service).
   - A customer fails to provide all required identifying information on an application or in response to notification that the application is not complete.

3. Unusual Use of, or Suspicious Activity Related to, the Covered Account:
   - The City is notified that the customer is not receiving their bill
   - The City is notified of unauthorized charges or transactions in connection with a customer's account.
   - Mail sent to a customer is repeatedly returned
   - An 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.)

4. Notice Regarding Possible Identity Theft:
   - The City receives notice from law enforcement officials, customers, or any other person regarding possible identity theft.

Detection of Red Flags

The City shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account

2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Response to Detected Red Flags

In the event that any City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Monitor a covered account for evidence of identity theft
2. Contact the customer
3. Reopen a covered account with a new account number
4. Not open a new covered account
5. Close an existing covered account
6. Notify law enforcement
7. Determine that no response is warranted under the particular circumstances.

UPDATING THE PROGRAM

The Program, including relevant Red Flags, is to be updated as often as necessary but at least annually to reflect changes in risk from Identity Theft.

PROGRAM ADMINISTRATION

Oversight Development, implementation, administration and oversight of this program will be the responsibility of the City Comptroller. The City Comptroller will be responsible for ensuring appropriate training of employees, for reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft.

Staff Training and Reports. Employees responsible for implementing this program shall be trained either by or under the direction of the City Comptroller in the detection of red flags and the responsive steps to be taken when a red flag is detected.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The City will take steps to ensure any service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

OTHER PROGRAMS AND POLICIES

This Policy incorporates herein the following other programs and policies established by the City in order to protect the identity of persons doing business with the City of Urbana and its employees as follows:

1. Software Programs managed and maintained by the City's Information Services office which programs are designed to protect confidential information maintained by the City of Urbana whether from City employees, customers or others doing business with the City.

2. Policies and practices developed pursuant to other state and federal laws such as the Health Insurance Portability and Accountability Act of 1996 and privacy rules developed thereunder.

3. Illinois Common Law and Privacy protections afforded pursuant to the Illinois Freedom of Information Act.

4. The Illinois Personal Identification Protection Act

5. Illinois Identity Theft Law

6. City of Urbana Personal Information Protection Policy (attached)

PERSONAL INFORMATION PROTECTION POLICY

WHEREAS, the State of Illinois has enacted a Personal Information Protection Act (815 ILCS 530/1 et seq.); and

WHEREAS, the disclosure of personal information may result in identity theft which is prohibited by Illinois law (720 ILCS 5/16 G-1 seq.); and

WHEREAS, it is appropriate to develop a written policy to protect against the unintentional or inadvertent disclosure of protected personal information.

NOW, THEREFORE, the following Personal Information Protection Policy is hereby promulgated:

1. Purpose. The purpose of this policy is to identify protected personal information and establish operating policies and procedures to protect against the inadvertent disclosure of protected personal information.

2. Protected Personal Information. As used herein shall include the following information whether stored in electronic or printed format and whether belonging to any customer, employee or contractor:

A. Credit card information including the following:

1. Credit card number
2. Credit card expiration date
3. Three (3) digit security code
4. Cardholder name
5. Cardholder address

B. Tax identification numbers:

1. Social Security number
2. Business identification number
3 Employer identification number

C. Payroll information including:

1. Paychecks
2. Pay stubs
3. Tax form

D. Cafeteria plan associated paperwork

E. Medical information including but not limited to:
   1. Doctor names
   2. Insurance claims
   3. Prescriptions
   4. Any related personal medical information

F. Other personal identifiers including:

   1. Date of birth
   2. Address
   3. Phone number
   4. Maiden name
   5. Name
   6. Customer number
   7. Driver's license number or state ID card identification card number
   8. Employment identification number

G. Codes and passwords including:

   1. Security codes
   2. Access codes or passwords to access to financial accounts or City property or information systems
   3. Personal identification numbers (PINs)
   4. Electronic identification numbers

3. City employees are encouraged to use commonsense judgment in securing protected personal information. If an employee is uncertain of the sensitivity of a particular piece of information, the employee should contact a supervisor for direction. The following policies are designed to guide employees in handling and securing protected personal information.

A. File cabinets, desk drawers, overhead cabinets and any other storage space containing documents with protected personal information will be locked when not in use.

B. Storage rooms containing documents with personal protected information and record retention areas will be locked at the end of each work day or when unsupervised.

C. Desks, work stations, work areas, printers and fax machines and common-shared work areas will be cleared of all documents containing protected personal information when not in use.

D. Whiteboards, dry erase boards, writing tablets, et cetera in common-shared work areas will be erased, removed or shredded when not in use.

E. When documents containing protected personal information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanic cross-cut or Department of Defense approved shredding device. Locked shred bins are labeled "confidential paper shredding and recycling". Municipal records, however, may only be destroyed in accordance with the State of Illinois Records Retention Policy.

F. Protected personal information may be transmitted using approved municipal email. All protected information must be encrypted when stored in electronic format.

G. Any protected personal information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as the following shall be included in the email: This message may contain confidential and/or priority information and is intended for the person/entity to which it was originally addressed. Any use by others is strictly prohibited.

H. When discarding devices that contain protected personal information stores in an electronic format, the protected personal information shall be destroyed or whipped clean so that the protected personal information is either unintelligible or destroyed.

4. Exceptions. This policy shall not prohibit the following:

A. The capture or transmission of protected personal information in the ordinary and lawful course of business of the City of Urbana.

B. The use of protected personal information by a peace officer, court office or other law enforcement personnel whether federal, state, or local while in the lawful performance of official duties.

C. The disclosure of protected personal information as allowed pursuant to the Illinois Freedom of Information Act, the Illinois Open Meeting Act or any other applicable law or court order.