ITEM #____36____
DATE__04-14-09

COUNCIL ACTION FORM

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM

BACKGROUND:

Recent modifications to the Fair and Accurate Credit Transactions Act of 2003 (FACT) administered by the Federal Trade Commission (FTC) require that all public utilities formally establish and maintain an Identity Theft Prevention Program. The intent of the program is to help prevent, detect, and mitigate identity theft by establishing a process to identify and report transactions that indicate a pattern, practice, or specific activity of the possible existence of identity theft. Required elements of the program include:

- The utility must conduct a needs assessment and implement improvements based on the assessment.

- After conducting the needs assessment, the utility must establish a written Identity Theft Prevention Program to be approved by the City Council.

- A Privacy Committee must be formed and a Privacy Officer designated. The Privacy Committee is responsible for oversight and reporting on implementation of the Identity Theft Prevention Program.

A privacy committee has been established consisting of:

Mike Wheelock, Utility Customer Services Supervisor
Duane Pitcher, Director of Finance, Program Administrator
Stan Davis, Information Technology Manager
Sue Rybolt, Assistant Director of Finance
Matt Duncan, Police Officer
Roger Wisecup, City Treasurer, Privacy Officer

This group has extensive experience and knowledge of utility transactions, fraud detection, electronic financial processing, and identity theft. The group has begun work conducting a needs assessment and has drafted an Identity Theft Prevention Program. The recommended plan was based on FTC guidelines, training conducted by the American Public Power Association, information provided by the Iowa Association of Public Utilities, and specific information related to the City of Ames. This group believes that the draft program meets all the requirements of applicable federal regulations.

The next step in compliance is Council approval of the program. The program is required to be in place by May 1, 2009. Therefore, any changes made by Council will need to be incorporated and approved at the April 28, 2009 Council meeting.

ALTERNATIVES:

1. Adopt the City of Ames Identity Theft Prevention Program.

2. Direct staff to make modifications to the Identity Theft Prevention Program to be brought back to the Council for approval on April 28, 2009.

.

MANAGER'S RECOMMENDED ACTION:

Adoption of an Identity Theft Prevention Program is required by the Federal Trade Commission for all public utilities and will provide a valuable service to the customers of the utility. The attached program accomplishes these purposes.

Therefore, it is the recommendation of the City Manager that the City Council adopt Alternative No. 1, thereby adopting the City of Ames Identity Theft Prevention Program.

City of Ames, Iowa
Identity Theft Prevention Program
Proposed for Adoption April 14, 2009

This Identity Theft Program was adopted by the City of Ames, Iowa pursuant to the Federal Trade Commission's (FTC) Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. 16 C. F. R. § 681.2.

I. PROGRAM ADOPTION

The Program was developed with oversight and approval of the Privacy Committee (defined below). After consideration of the size and complexity of the City's operations and customer account systems, and the nature and scope of the City's activities, the Privacy Committee determined that this Program was appropriate for the City of Ames, Iowa and therefore submitted the Program for approval by the City Council on April_____, 2009.

II. PROGRAM PURPOSE

The City of Ames, Iowa developed this Identity Theft Prevention Program to help protect customers of the City'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 and maintenance of certain utility accounts. The Program does so by identifying "red flags" that suggest or indicate the possibility of identity theft and providing guidelines on how the City should respond once it detects any such red flags.

III. PRIVACY COMMITTEE

The Privacy Committee is responsible for the development, implementation, and administration of the City's Identity Theft Prevention Program. The Privacy Committee will be composed of the following individuals: Director of Finance designated as the Program Administrator, Investment Officer/Treasurer designated as the Privacy Officer, Assistance Director of Finance, IT Manager, Utility Accounts Supervisor, and a Law Enforcement Officer appointed by the Chief of Police.

IV. PROGRAM DEFINITIONS

A. **City** means City of Ames, Iowa.

B. **Covered Account** means 1) an account the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and 2) any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft.
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.
D. **Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for extension, renewal, or continuation of credit; or any assignee or an original creditor who participates in the decision to extend, renew, or continue credit, including utility companies.
E. **Customer** means a person that has a covered account with a creditor.
F. **Identity Theft** means a fraud committed or attempted using the identifying information of another person without authority.
G. **Identifying Information (Sensitive Information)** means any name or number that may be used to identify a specific person including, but not limited to name, date of birth, driver's license number, Social Security number, student identification number, passport number, credit card account information; debit card account information, or bank account information.
H. **Impacted Employee** means any employee who performs any activity in connection with one or more covered accounts.
I. **Person** means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
J. **Program** means the City of Ames, Iowa's Identity Theft Prevention Program.
K. **Red Flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
L. **Service Provider** means a person that provides a service directly to the City.
M. **SSN** means social security number.

V. IDENTIFICATION OF RED FLAGS

In order to identify relevant red flags, the City considered the types of accounts it offers and maintains, the methods it provides to open accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The City identifies the following red flags, in each of the listed categories:

A. **Notifications And Warnings From Consumer Reporting Agencies**

- The City does not report to or obtain information from consumer reporting agencies, so it did not identify any relevant red flags for this category.
- If the City begins to report to or obtain information from a consumer reporting agency, then the Privacy Committee will consider the following as possible red flags for this category: 1) receiving a report or notice from a consumer reporting agency of a credit freeze; 2) receiving a report of fraud with a consumer report; and 3) receiving indication from a consumer report of activity that is inconsistent with a customer's usual pattern or activity.

B. **Suspicious Documents**

- Identification document or card provided for identification that appears to be forged, altered or inauthentic.

- Identification document or card on which the person's photograph or physical description is not consistent with the appearance of the person presenting the identification.
- Identification document or card on which information is not consistent with other information given by the applicant.
- Application for service that appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

C. **Suspicious Personal Identifying Information**
- A person's identifying information is inconsistent with other sources of information (such as an address not matching an address on a consumer report or an SSN that was never issued or is listed in the Social Security Administration's death master file).
- A person's identifying information is inconsistent with other information the customer provides (such as inconsistent SSNs or birth dates).
- A person's identifying information is the same as shown on other applications found to be fraudulent.
- A person's identifying information is associated with known fraudulent activity (such as a fictitious or prison mailing address or an invalid telephone number).
- A person's SSN is the same as another customer's SSN.
- A person's address or telephone number is the same as that of another person.
- A person fails to provide complete personal identifying information on an application when requested to do so.
- A person's identifying information is not consistent with the information that is on file for the customer.

D. **Unusual Use Of Or Suspicious Activity Related To An Account**
- A change of mailing address on an account followed by a request to start an additional service at another location or to add another authorized user to the account.
- Payments are made in a manner associated with fraud (such as deposit or initial payment made and no further payments).
- An account being used in a way that is not consistent with prior use (such as late or no payments when the account has been timely in the past).
- An account with low usage unexpectedly jumps to high consumption (take into consideration the type of account, expected pattern of usage and other relevant factors).
- Mail sent to the account holder is repeatedly returned as undeliverable.
- City receives notice that a customer is not receiving his paper statements (the City is considering offering electronic billing).
- City receives notice that an account has unauthorized activity.

E. **Notice Regarding Possible Identity Theft**
- City notified by a customer, law enforcement or another person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

VI. DETECTION OF RED FLAGS

The employees of the City that interact with residents/customers shall have the initial responsibility for monitoring the information and documentation provided by residents/customers in connection with the opening of new accounts or modifying existing accounts for red flags. The Privacy Officer

is responsible for ensuring all employees are trained so they are able to recognize the relevant red flags identified in this Program.

A. **New Covered Accounts**
In order to detect any of the red flags identified in section V above related to the opening of a new covered account, City personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Requiring certain identifying information such as name, date of birth, residential or business address, SSN, driver's license or other identification.
- Verifying the customer's identity by reviewing a driver's license or other identification card.
- Independently contacting the customer.

B. **Existing Covered Accounts**
In order to detect any of the red flags identified in section V above related to an existing covered account, City personnel will take the following steps to monitor transactions:

- Verify the identification of customers if they request information.
- Verify the validity of requests to change mailing address.
- Verify changes in banking information given for billing and payment purposes.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

A. **Securing Sensitive Information**
Employees are expected to use good judgment in securing sensitive information. If an employee is uncertain of the sensitivity of a particular piece of information, the employee should contact their supervisor or the Privacy Officer. Request for sensitive information or documents under the Iowa Open Records Law shall be forwarded to the Privacy Officer.

In order to further reduce the likelihood of identity theft occurring with respect to City accounts, the City shall make reasonable efforts to comply with the following steps related to its internal operating procedures:

- Require and keep only the kinds of sensitive information that are necessary for City purposes.
- File cabinets containing documents with sensitive information shall be inaccessible to unauthorized individuals and shall be locked or kept in a locked room during nonworking hours.
- Ensure complete and secure destruction of paper documents and computer files containing sensitive information.
- Restrict access to the sensitive information on the Customer Information System to employees authorized by the Privacy Officer.
- Authorized employees will not leave their computer unattended when they are signed on to the Customer Information System. They must sign out of the Customer Service Information system or leave it attended by another authorized user.
- At employee work stations, computer screens displaying, or papers containing sensitive information will be positioned in such a way that unauthorized individuals cannot view the information.
- Ensure the City’s website is secure or provide clear notice that the website is not secure.
- Ensure computer virus protection is up-to-date.

B. **Reponses When Red Flags Are Detected**

If an employee detects a red flag indicating possible identity theft with respect to opening a new covered account or to an existing covered account, the employee shall use his/her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his/her discretion, the employee determines that identity theft (or attempted theft) is likely or probable, the employee shall report such red flags to the Privacy Officer. If the employee determines that identity theft is unlikely or reliable information is available to reconcile red flags, the employee shall report this information to the Utility Accounts Supervisor.

In the event City personnel detect any identified red flags, they shall also take one or more of the following steps, depending on the degree of risk posed by the red flag:

- Continue to monitor an account for evidence of identity theft.
- Contact the customer.
- Change any passwords or other security devices that permit access to covered accounts.
- Request additional identifying information from the applicant.
- Decline or refuse to open a new covered account.
- Reopen an account with a new number.
- Close an existing covered account.
- Notify law enforcement.
- Determine that no response is warranted under the particular circumstances.

VIII. SERVICE PROVIDER ARRANGEMENTS

The following steps will be taken related to a service provider agreement if a service provider performs an activity for the City in connection with one or more covered accounts.

A. **For Existing Service Provider Agreements**

The Program Administrator shall exercise his/her discretion in reviewing such agreements in order to ensure, to the best of his/her ability, that the service provider's activities are conducted in accordance with policies and procedures designed to detect any red flags that may arise in the performance of a service provider's activities and take appropriate steps to prevent or mitigate identity theft.

B. **For Service Provider Agreements Entered Into After The Adoption Of The Program**

The Program Administrator shall exercise his/her discretion in reviewing such agreements in order to ensure, to the best of his/her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, designed to detect any red flags that may arise in the performance of a service provider's activities, and take appropriate steps to prevent or mitigate identity theft. The service provider shall be required, by contract, to report incidents of identity theft involving any covered account of the City.

IX. PROGRAM ADMINISTRATION

A. **Oversight**

- The Program Administrator is responsible for developing, implementing, administering, and providing operational oversight of the Program.

- The Privacy Officer is responsible for ensuring that impacted employees are trained in the policies and the procedures related to this Program, determining which steps of prevention and mitigation should be taken in particular circumstances, and reviewing staff reports regarding the detection of red flags and the steps taken to prevent or mitigate identity theft.
- The Privacy Committee is responsible for assisting the Program Administrator and Privacy Officer in the performance of their duties and responsibilities.

B. **Updating The Program And The Red Flags**

The Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City from identity theft. At least every six months, the Privacy Committee will meet to consider the City's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the City maintains, and changes in the City'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 changes are warranted, the Program Administrator will present the City Council with his/her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

C. **Staff Training**

Impacted employees shall be trained by or under the direction of the Privacy Officer in the detection of red flags and the responsive steps to be taken when red flags are detected. Impacted employees shall be trained in the program upon hire or whenever the program is updated. The Privacy Officer shall provide impacted employees with annual training reviews to reinforce the importance of the Program.

D. **Reports**

- At least every 6 months, the Privacy Officer shall submit a report to the Privacy Committee summarizing any incidents of identity theft detected, prevented or mitigated by employees and an evaluation of the City's compliance with the Program.
- On annual basis, the Program Administrator shall submit to the City Council a report on the City's compliance with the Program and evaluation of issues such as: 1) the effectiveness of the procedures and practices of the City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing accounts; and 2) significant incidents involving identity theft and the City's response.

X. SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY

This Program is to be adopted by a public body and thus made publicly available. The City recognizes that to be effective, there is a need for a level of confidentiality regarding the City's specific procedures and practices relating to identity theft detection, prevention and mitigation. Therefore, only the Program's general red flag detection, prevention, and mitigation procedures and practices are listed in this document. Under this Program, knowledge of specific procedures and practices is limited to the Privacy Committee and those employees who need to know for the purpose of detecting, preventing, and mitigating identity theft.