CHAPTER 19

ILLINOIS/FEDERAL MANDATED POLICIES

ARTICLE I – IDENTITY THEFT PREVENTION POLICY

19-1-1 COMPLIANCE WITH FEDERAL LAW. The City is committed to comply with the Federal Fair and Accurate Credit, Transactions Act of 2003, as well as provide customers, particularly customers with utility accounts, the maximum identity theft protection possible. Situations that lead to identity theft would hurt and inconvenience the City's customers, while at the same time damage the City's reputation and place the City at risk for losses. The City developed this Identity Theft Prevention Policy with the oversight and approval of the City Council after considering the size and complexity of the City's operations and account systems and the nature and scope of the City's activities.

(A) **Examples of Identity Theft.**

(1) An identity thief uses another person's social security number to open a utility account.

(2) An identity thief uses a victim's information to obtain unauthorized services from the City.

(3) An identity thief opens a utility account using a victim's name and good credit.

(4) An identity thief files for bankruptcy using a victim's name.

(5) An identity thief gives a victim's name as his/her own when arrested by police.

19-1-2 RISK ASSESSMENT/IDENTIFYING RELEVANT RED FLAGS. While the overall risk of identity theft involving the City appears low, the City will focus on detection and prevention from identity theft on the following covered accounts: accounts to individual customers; all of the City's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial; any account the City offers or maintains primarily for personal, family or household purposes that involves multiple payments or transactions; and any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from Identity Theft, as well as automatic deposits to the accounts of the City employees. There will be a periodic review to determine if the covered accounts are still accurate due to any changes such as changes of address or other changes which may occur relating to an account.

Each type of covered account will be examined and reviewed for relevant Red Flags in part by considering:

(A) The methods provided to open covered accounts;

(B) The methods provided to access covered accounts; and

(C) Previous experiences with identity theft.

As part of the process, the City will consider the relevant Red Flags provided by the regulatory guidance, as well as incidents of identity theft that the City and/or the City customers have experienced and applicable supervisory guidance.

19-1-3 DETECTED RED FLAGS. The City is committed to detecting situations in which identity theft might have or may have occurred.

A "Red Flag" is a pattern, practice or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the City considered risk factors such as the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts and its previous experiences with Identity Theft.

Identity Theft will be combated by detecting Red Flags in connection with the opening of covered accounts, and existing covered accounts, such as by:

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

(B) Authenticating customers' transactions, including photo ID if necessary, plus possible additional verification methods such as a user ID and password.

(C) Monitoring transactions with emphasis on a change of address closely followed by a new service request or a material change in a customer's credit use.

(D) Verifying the validity of change of address requests in the case of existing covered accounts in order to monitor the diversion of statements as a prelude to possible account manipulation.

19-1-4 PREVENTING AND MITIGATING IDENTITY THEFT. In order to prevent and mitigate Identity Theft, the City will provide appropriate responses to the following Red Flags:

(A) **Alerts, Notifications or Warnings from a Consumer Reporting Agency.**

(1) A fraud or active duty alert is included with a credit report.

(2) A credit reporting agency provides a notice of credit freeze in response to a request for a credit report.

(3) A credit reporting agency provides a notice of address discrepancy.

(4) Receiving a report of fraud with a credit report.

(5) Receiving indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

(B) **Suspicious Documents.**

(1) Documents provided for identification appear to have been altered, forged or unauthentic.

(2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or person presenting the identification.

(3) Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged).

(4) Receiving an application for service that appears to have been altered or forged.

(C) **Suspicious Personal Identifying Information.**

(1) The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

(2) Personal identifying information provided is not consistent with personal identifying information that is on file with the City.

(3) A person's identifying information is the same as shown on other applications found to be fraudulent.

(4) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).

(5) A person's social security number is the same as another customer's social security number.

(6) A person's address or phone number is the same as that of another person.

(7) A person's identifying information is not consistent with other information the customer provides.

(D) **Unusual Use of, or Suspicious Activity Related to the Covered Account.**

(1) A change of address for a covered account followed by the City receiving a request for the addition of authorized users on the account or adding other parties.

(2) A covered account that has been inactive and then becomes active.

(3) Payments stop on an otherwise consistently up-to-date account.

(4) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

(5) The City is notified of unauthorized charges or transactions in connection with a customer's covered account.

(6) A new account is used in a manner consistent with fraud (such as the customer failing to make the first payment, or making the initial payment and no other payments).

(5) 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).

(6) The City receives notice that a customer is not receiving his/her paper statements.

(E) **Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities and/or Other Persons Regarding, Possible Identity Theft in Connection with Covered Accounts Held by the City.**

(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.

(2) Should any of the above instances of suspicious activity that could be identity theft occur, the City will take immediate actions to either prevent or investigate the situation.

In order to detect any of the Red Flags identified above with the opening of a new account, City personnel will take the following steps to obtain and verify the identity of the person opening the account:

Steps can include:

(a) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, social security number, driver's license or other identification.

(b) Verifying the customer's identity, such as by copying and reviewing a driver's license or other identification card.

(c) Reviewing documentation showing the existence of a business entity.

(d) Independently contacting the customer.

In order to detect any of the Red Flags identified above for an existing account, City personnel will take the following steps to monitor transactions with an account:

Steps can include:

(a) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via e-mail).

(b) Verifying the validity of requests to change billing addresses.

(c) Verifying changes in banking information given for billing and payment purposes.

Responses to these Red Flags are commensurate with the degree of risk posed based on the City's risk assessment.

Appropriate responses may include the following:

(a) Complete verification of identification for fraud, active duty, credit freeze or address discrepancy alert for any of these types of alerts found on a consumer credit report when applying for services;
(b) Monitoring a covered account for evidence of identity theft or suspicious activity by placing on the City's watch list;
(c) Contacting the customer;
(d) Changing any passwords, security codes, or other security devices that permit access to a covered account;
(e) Reopening a covered account with a new account number;
(f) Not opening a new covered account;
(g) Closing an existing covered account;
(h) Not attempting to collect on a covered account or not sending a covered account to a debt collector;
(i) Notifying law enforcement; or
(j) Determining that no response is warranted under the particular circumstances.

19-1-5 DUTIES REGARDING CHANGE OF ADDRESS. If a notice of change of address for an existing account is received and then within **thirty (30) days** a request for a change to the account is made, the City will assess the validity of the change of address or requested change to the account.

19-1-6 UPDATING THE PROGRAM. The City will periodically review and update this policy (including the Red Flags determined to be relevant) to reflect changes in risks to customers or to the safety and soundness of the City from identity theft, based on factors such as:

(A) Experiences with identity theft;
(B) Changes in methods of identity theft;
(C) Changes in methods to detect, prevent, and mitigate identity theft;
(D) Changes in the types of accounts or services that the City offers or maintains; and
(E) Changes in our business arrangements, including services provided and service provider arrangements.

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 update the Program or present the City Council with his or her recommended changes, and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

19-1-7 PROGRAM ADMINISTRATION.

(A) The ultimate oversight of the program is the City Council. The City Council has assigned specific responsibility for the Program's implementation to the Program Administrator, designated by the City Council to be the City Clerk.

(B) The Program Administrator will report to the City Council, at least annually, on compliance by the City with all identity theft issues.

(C) The report will address material matters related to the Program and evaluate issues such as:

(1) The effectiveness of the policies and procedures of the City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

(2) Service provider arrangements;

(3) Significant incidents involving identity theft and management's response; and

(4) Recommendations for material changes to the Program.

The City Council will take any additional steps necessary to support this program.

19-1-8 SERVICE PROVIDER ARRANGEMENTS. The City will oversee any service provider who performs an activity in connection with one or more covered accounts. The City will 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 and require the service provider to report any Red Flag to the Program Administrator.

19-1-9 TRAINING. The City staff responsible for implementing the Program will be trained to recognize and detect Red Flags and properly react to unauthorized or fraudulent attempts to obtain customer information. The City directs the Program Administrator to conduct annual training for all employees regarding identity theft and to supplement that training throughout the year as more schemes are uncovered.

19-1-10 EDUCATION OF CUSTOMERS. Educating consumers about preventing identity theft and identifying potential pretext calls may help reduce their vulnerability to these fraudulent practices. The City will have brochures available to consumers and an identity theft prevention section on the City's website that describes preventative measures consumers can take to avoid becoming victims of these types of fraud.

19-1-11 OTHER APPLICABLE LEGAL REQUIREMENTS. As part of the overall Program, the City will include other legal requirements when needed, such as:

(A) Filing a Suspicious Activity Report; and

(B) Implementing any requirements under which accounts may be created, changed or altered when the City detects a fraud or active duty alert.

19-1-12 ASSISTANCE FOR VICTIMS. In the event one of the City's customers becomes a victim of identity theft, the following steps will be taken, as appropriate, to assist the customer:

(A) Have trained personnel respond to customer calls regarding identity theft or pretext calling.

(B) Determine if it is necessary to close an account immediately after a customer reports unauthorized use of that account and create a new customer account when appropriate.

(C) Where a customer has multiple accounts, an assessment will be made as to whether any other account has been the subject of potential fraud.

(C) Help educate the customer about appropriate steps to take if the customer has been victimized.

(Ord. No. 2008-10-01; 11-10-08)