CITY OF MARQUETTE, MICHIGAN

CITY COMMISSION POLICY

Policy Number: **2008-02**	
Date Adopted: October 27, 2008	
Department: Administrative	

SUBJECT: **IDENTITY THEFT PREVENTION PROGRAM**

I. OBJECTIVE:

A. To protect the identity and personal financial data of utility customers and to minimize the possibility of identity theft of customer information.

B. To comply with the FACT Act of 2003 and the requirements of the Federal Trade Commission and their "Red Flags" Rules as published in the *Federal Register* on November 9, 2007.

C. To establish a program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing account.

II. SCOPE: This program applies to all employees of the City of Marquette.

III. POLICY:

A. The Finance Director and City Treasurer will be responsible for ongoing involvement in the development, implementation and administration of the Identity Theft Prevention Program.

B. Training for employees who handle sensitive personal information will be provided as necessary.

C. Oversight of third party service providers will assure that they also comply with the Program.

D. A written annual report will be made and presented to the City Manager regarding compliance with the Program and any incidents experienced for the year. The report will include:

a. The effectiveness of the policies and procedures in addressing the risk of identity theft;
b. Significant incidents that have occurred and management's response; and
c. Recommendations for changing the Program.

E. As risk factors are discovered, such as identity theft, customer information breach, etc., the program will be revised to address any future risks.

F. An investigation will be conducted when any of the following "Red Flags" are discovered. They may include but are not limited to:
   a. Incidents of identity theft;
   b. Methods of identity theft that reflect identity theft risks;
   c. Alerts, notifications, or other warnings received from a consumer reporting agency or third party service provider;
   d. The presentation of suspicious documents, such as those suspected to be altered or forged;
   e. The presentation of suspicious personal identification information;
   f. The unusual use of an account;
   g. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft;
   h. Identification photo that does not match the person; and
   i. Mail sent to a customer that is frequently returned.

G. When setting up a new customer or changing an address for an existing customer, every effort shall be made to verify all information given.

H. Monitoring the security of customer identity data must be an ongoing process. When it is determined that a customer's information has been jeopardized, the following procedure will be followed:
   a. Contact the customer(s);
   b. Notify upper management;
   c. Take immediate steps to eliminate the cause of the breach of information; and
   d. Notify law enforcement if the situation warrants.

I. The Finance Director and City Treasurer will provide ongoing oversight of third party software providers and service providers that utilize customer information to assure that customer identity information is secure and utilized properly.

IV. PROCEDURES:

Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

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: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

Covered account means:

A. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, cell phone accounts, **utility accounts**, checking accounts and savings accounts; and
B. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Identification of Red Flags:

A. Suspicious Documents
    a. Identification document or card that appears to be forged, altered or not authentic;
    b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
    c. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
    d. Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information
    a. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
    b. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on the utility records);
    c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
    d. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
    e. An address or phone number presented that is the same as that of another person;
    f. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and

g. A person's identifying information is not consistent with the information that is on file for the customer.

C. Suspicious Account Activity or Unusual Use of Account
   a. Change of address for an account followed by a request to change the account holder's name;
   b. Payments stop on an otherwise consistently up-to-date account;
   c. Account used in a way that is not consistent with prior use (example: very high activity);
   d. Mail sent to the account holder is repeatedly returned as undeliverable;
   e. Notice to the City that a customer is not receiving mail sent by the City;
   f. Notice to the City that an account has unauthorized activity;
   g. Breach in the City's computer system security; and
   h. Unauthorized access to or use of customer account information.

D. Alerts from Others - Notice to the City from a customer, identity theft victim, law enforcement or other person that the City has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detecting Red Flags:

E. New Accounts. In order to detect any of the Red Flags identified above associated 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:
   a. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
   b. Verify the customer's identity (for instance, review a driver's license or other identification card);
   c. Review documentation showing the existence of a business entity; and/or
   d. Independently contact the customer.

F. Existing Accounts. 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:
   a. Verify 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; and
   c. Verify changes in banking information given for billing and payment purposes.

Responding Appropriately to Any Red Flags Detected:. In the event 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:

G. Prevent and Mitigate
    a. Continue to monitor an account for evidence of Identity Theft;
    b. Contact the customer;
    c. Change any passwords or other security devices that permit access to accounts;
    d. Not open a new account;
    e. Close an existing account;
    f. Reopen an account with a new number;
    g. Notify the City Treasurer or Finance Director for determination of the appropriate step(s) to take;
    h. Notify law enforcement; and/or
    i. Determine that no response is warranted under the particular circumstances.

H. Protect customer identifying information
    a. Ensure complete and secure destruction of paper documents and computer files containing customer information;
    b. Keep the work station clean and offices clear of papers containing customer information;
    c. Secure the work station by logging off or locking the computer whenever leaving the workstation for lunch or extended periods of time.
    d. Do not request social security numbers;
    e. Require and keep only the kinds of customer information that are necessary for utility purposes; and
    f. Prevent customers from eavesdropping on other customers transacting business at the customer service counter.

Program Updates: This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City from Identity Theft. The Finance Director and City Treasurer will consider the City's experiences with Identity Theft situations, 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 Finance Director and City Treasurer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Finance Director and City Treasurer will present the City Manager with recommended changes and the City Manager will make a determination of whether to accept, modify or reject those changes to the Program.

Program Administration:

I. Oversight. The Finance Director and City Treasurer will be responsible for developing, implementing, updating, and administering the Program as well as for ensuring appropriate training of City staff 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 and considering periodic changes to the Program.

J. Staff Training and Reports. City staff responsible for implementing the Program shall be trained either by or under the direction of the Finance Director or City Treasurer in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. City staff is required to provide reports to the Finance Director and City Treasurer on incidents of Identity Theft, the City's compliance with the Program and the effectiveness of the Program.

K. Specific Program Elements and Confidentiality. For the effectiveness of Identity Theft prevention Programs, the Red Flags Rules envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Finance Director and City Treasurer and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.

V. RESPONSIBILITY**:** The Finance Director and City Treasurer are responsible for the administration of this program.