IDENTITY THEFT PREVENTION

1. Purpose

This regulation is to establish an identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with the Federal Trade Commission's Red Flag Rule (part 681 of Title 16 of the Code of Federal Regulations) implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Under the Red Flags Rule, every financial institution and creditor **(including utilities)** is required to establish an "identity theft prevention program" tailored to its size, complexity, and the nature of its operation. Each program must contain reasonable policies and procedures to:

A. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the Program;

B. Detect red flags that have been incorporated into the Program;

C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

D. Insure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft.

2. Definitions

Identity 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 tax payer identification number, unique electronic identification number, computer's internet protocol address or routing code.

A covered account means:

1) 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, automobile loans, margin accounts, cell phone accounts, and **utility accounts**, checking accounts, and savings accounts; and

2) 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 a financial institution or creditor from identity theft, including financial, operational compliance, reputation or litigation risks.

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

3. Policy

A. IDENTIFICATION OF RED FLAGS

The City of Port Huron identifies the following red flags, in each of the listed categories:

1) Suspicious documents

a) Identification document or card that appears to be forged, altered or inauthentic;
b) Identification document or card in 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.

2) 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 a credit report or other information available);
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) Social security number presented that is the same as one given by another customer;

f) An address or phone number presented that is the same as that of another person;
g) 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
h) A person's identifying information is not consistent with the information that is on file for the customer.

3) 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.

4) Alerts from others

a) Notice to the City from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account or investigation for a person engaged in identity theft.

B. **ACCOUNTS**

1) 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 identify 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, driver's license or other identification;
b) Verify the customer's identity (for instance, review a driver's license or other identification card); and
c) Review documentation showing the existence of a business entity; and/or
d) Independently contact the customer.

2) 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 a customer 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.

C. PREVENTING AND MITIGATING IDENTITY THEFT

In the event that 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) Prevent and mitigate
   a) Continue to monitor an account for evidence of identify 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 Finance Director and City Attorney 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.

2) Protect customer identifying information. In order to further prevent the likelihood of identity theft with respect to City accounts, the City will take the following steps with respect to its internal operating procedures to protect the customer identifying information:

   a) Insure that its website is secure of provide clear notice that the website is not secure;
   b) Insure complete and secure destruction of paper documents and computer files containing customer information;
   c) Insure that office computers are password protected and that computer screens locked after a set period of time;
   d) Keep offices clear of papers containing customer information;
   e) Request only the last four digits of social security numbers (if any);
   f) Insure computer virus protection is up to date; and
   g) Require and keep only the kinds of customer information that are necessary for utility purposes.

D. PROGRAM REVIEW

This program will be periodically reviewed and updated to reflect changes and risk to customers and the soundness of the City from identity theft. The City Manager or his designee 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 City Manager or his designee will determine whether changes to the Program including the listing of red flags are warranted. If warranted, the City Manager will make a determination of whether to accept, modify or reject those changes to the Program.

E. **PROGRAM ADMINISTRATION**

1) Oversight. Responsibility for developing, implementing, and updating this Program lies with an identity theft committee for the City. The committee is headed by the Finance Director with a police department detective assigned by police administration and the City Attorney comprising the remainder of the committee membership. The City Finance Director will be responsible for the Program administration for insuring appropriate training of City staff of 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.

2) Staff training and reports. City staff responsible for implementing the Program shall be trained either by or under the direction of the City Finance Director 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 Program administrator on incidents of identity theft, the City's compliance with the Program, and the effectiveness of the Program.

3) Specific Program elements and confidentiality. For the effectiveness of identity theft prevention program the red flag rule 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 are to be limited to the identity theft committee 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 counter productive to list these specific practices here, therefore only the Program's general red flag detection implementation and prevention practices are listed in this document.

4) Authority and revisions. This policy is enacted immediately upon the approval of the City Manager and the adoption of the Program as an administrative regulation of the City. Revisions to this policy shall only be enacted when approved by the City Manager and adopted as an amended administrative regulation of the City. This policy shall be reviewed at least biennially by the identity theft committee for the City who shall make any recommendations for changes to the City Manager for updating the policy.