cityofnovi.org

CITY of NOVI CITY COUNCIL

Agenda Item I
October 20, 2008

SUBJECT: Approval of Policy for the Water & Sewer/Treasury Department Identity Theft Prevention Program

SUBMITTING DEPARTMENT: Finance/Legal

CITY MANAGER APPROVAL:

BACKGROUND INFORMATION:

Recently, the Federal Trade Commission adopted rules and guidelines to implement Sections 114 and 315 of the Federal Fair and Accurate Credit Transactions Act of 2003 (FACTA). These rules are referred to as the "Red Flag Rules," and essentially require "financial institutions and creditors" to adopt an Identify Theft Program to detect, prevent, and mitigate identity theft in connection with certain accounts. Until recently, it was unclear whether governmental entities fell within the category of creditors required to adopt such policies; however, it has been determined that any municipality that maintains utility billing accounts, even through a third party, or maintains any continuing account for which there is a foreseeable risk of identity theft, and because Novi's Water & Sewer Fund provides such services we recommend the attached policy.

RECOMMENDED ACTION: Approval of Policy for the Water & Sewer/Treasury Department Identity Theft Prevention Program

	1	2	Y	N
Mayor Landry				
Mayor Pro Tem Capello				
Council Member Crawford				
Council Member Gatt				

	1	2	Y	N
Council Member Margolis				
Council Member Mutch				
Council Member Staudt				

City of Novi
Water & Sewer/Treasury Department
OFFICIAL POLICY & PROCEDURE

TITLE:	EFFECTIVE DATE:
IDENTITY THEFT PREVENTION PROGRAM	**October 20, 2008**

Purpose

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 Flags 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 Flag Rule, every financial institution and creditor, including a municipality that maintains utility billing accounts, 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:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers/users or to the safety and soundness of the creditor from Identity Theft.

Definitions

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.

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

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, **utility accounts**, checking accounts and savings accounts; and

2. Any other account that a financial institution or creditor, or municipality, offers or maintains for which there is a reasonably foreseeable risk to customers/users or to the safety and soundness of the financial institution or creditor or municipality 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.

Policy

A. **IDENTIFICATION OF RED FLAGS**. The City identifies the following red flags, in each of the listed categories:

1. Suspicious Documents
   i. Identification document or card that appears to be forged, altered or inauthentic;
   ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
   iii. Other document with information that is not consistent with existing customer/user information (such as if a person's signature on a check appears forged); and
   iv. Direct Payment Enrollment Form that appears to be altered or forged.

2. Suspicious Personal Identifying Information
   i. Identifying information presented that is inconsistent with other information the customer/user provides (example: inconsistent birth dates);
   ii. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
   iii. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
   iv. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
   v. An address or phone number presented that is the same as that of another person;
   vi. A person's identifying information is not consistent with the information that is on file for the customer/user.

3. Suspicious Account Activity or Unusual Use of Account
   i. Change of address for an account followed by a request to change the account holder's name;
   ii. Payments stop on an otherwise consistently up-to-date account;
   iii. Account used in a way that is not consistent with prior use (example: very high activity);
   iv. Mail sent to the account holder is repeatedly returned as undeliverable;
   v. Notice to the City that a customer/user is not receiving mail sent by the City;
   vi. Notice to the City that an account has unauthorized activity;
   vii. Breach in the City's computer system security; and
   viii. Unauthorized access to or use of customer/user account information.

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

B. **DETECTING RED FLAGS.**

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 identity of the person opening the account:
   i. Require certain identifying information such as residential or business address;
   ii. Independently contact the customer/user.

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:
   i. Verify the identification of customers/users if they request information (in person, via telephone, via facsimile, via email);
   ii. Verify the validity of requests to change billing addresses; and
   iii. Verify changes in banking information, if any, given for billing and payment purposes. Updated Direct Payment Enrollment Form required.

C. **PREVENTING AND MITIGATING IDENTITY THEFT.**

1. **Prevent and Mitigate.** 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:

   i. Continue to monitor an account for evidence of Identity Theft;

ii. Contact the customer/user;
iii. Change any passwords or other security devices that permit access to accounts;
iv. Not open a new account;
v. Close an existing account;
vi. Reopen an account with a new number;
vii. Notify the City Manager (or his/her designee) for determination of the appropriate step(s) to take;
viii. Notify law enforcement; and/or
ix. Determine that no response is warranted under the particular circumstances.

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

i. Ensure that its website is secure or provide clear notice that the website is not secure;
ii. Ensure complete and secure destruction of paper documents and computer files containing customer/user information;
iii. Ensure that office computers are password protected and that computer screens lock after a set period of time;
iv. Keep offices clear of papers containing customer/user information;
v. Ensure computer virus protection is up to date; and
vi. Require and keep only the kinds of customer/user information that are necessary for utility purposes.

D. **PROGRAM UPDATES**. This Program will be periodically reviewed and updated to reflect changes in risks to customers/users and the soundness of the City from Identity Theft. The City Manager (or his/her designee), in conjunction with the Finance Director/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 City Manager (or his/her designee), with the assistance of the City Finance Director/Treasurer, will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the City Manager (or his/her designee),will present the City Council with his/her recommended changes and the Board 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 City Manager (or his designee), with the City Finance Director/Treasurer, Assistant City Treasurer and Water and Sewer Financial Services Manager comprising the remainder of the committee membership. The City Manager (or his/her designee) will be responsible for the Program administration, 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.

2. **Staff Training and Reports**. City staff responsible for implementing the Program shall be trained either by or under the direction of the City Manager (or his/her designee) 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 Programs, 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 is 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 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.

Authority & Revisions

This policy is enacted immediately upon approval of the City Council, as reflected in the regular meeting minutes dated October 20, 2008. Revisions to this policy shall only be enacted when approved by the City Council and reflected in the applicable meeting minutes. This policy shall be reviewed at least biennially by the City Manager (or his/her designee) and City Council will be updated as appropriate.

Revision History

Date	Revision #	Nature of Revision
10/20/08	00	Original document.