RESOLUTION NO. 2380-08

A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF WINDSOR ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Federal Trade Commission ("FTC") has adopted regulations requiring "creditors" with "covered accounts" to develop and implement by May 1, 2009, due to a six-month extension of the requirement, an identity theft prevention program that complies with those regulations; and

WHEREAS, the FTC considers a government entity to be a "creditor" where it defers payment for goods or services by its customers. As the Town provides water and water reclamation services to customers, and the customers do not pay for these services until after they have been provided, the adoption of an identity theft program is required; and,

WHEREAS, the Town Council desires to take action to comply with the applicable FTC regulations by adopting an identity theft prevention program.

NOW, THEREFORE BE IT RESOLVED that the Town Council of the Town of Windsor, adopts, and directs Town staff to implement the Town of Windsor Identity Theft Protection Program attached as Exhibit "A".

PASSED, APPROVED AND ADOPTED this 5th day of November 2008, by the following vote:

AYES:	**COUNCILMEMBERS ALLEN, GOBLE, PARKER, SALMON AND MAYOR FUDGE**
NOES:	**NONE**
ABSTAIN:	**NONE**
ABSENT:	**NONE**

Debora Fudge

DEBORA FUDGE, MAYOR

ATTEST:

Maria De La O

MARIA DE LA O, TOWN CLERK

Attachment: Exhibit "A"

Exhibit A

TOWN OF
WINDSOR

Town of Windsor

Identity Theft Prevention Program

Prepared in accordance with the
Fair and Accurate Credit Transaction Act of 2003

Approved by Resolution No. 2380-08 of the Town Council on November 5, 2008

I. PROGRAM ADOPTION

The Town of Windsor ("Town") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the Administrative Services Director. After consideration of the size and complexity of the Town's operations and account systems, and the nature and scope of the Town's activities, the Administrative Services Director determined that this Program was appropriate for the Town of Windsor, and therefore the Town Council approved this Program on November 5, 2008.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, the Town is required to establish an "Identity Theft Prevention Program" ("Program") tailored to the Town's size, complexity and the nature of its operation. The 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 or to the safety and soundness of the creditor from Identity Theft.

The Town places the highest priority on protecting any confidential financial and personal information submitted to it in the course of providing Town services. The Program listed herein satisfies the Red Flag Rule requirements.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

According to the Rule, the Town is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

All the Town's accounts that are individual Town service accounts held by customers of the Town whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Town offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Town offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Town from Identity Theft.

"Identifying information" is defined under the Rule as "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.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Town considers 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. The Town identifies the following red flags, in each of the listed categories:

A. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. 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
4. Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. An address or phone number presented that is the same as that of another person;
6. 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
7. 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

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Town that a customer is not receiving mail sent by the Town;
6. Notice to the Town that an account has unauthorized activity;
7. Breach in the Town's computer system security; and
8. Unauthorized access to or use of customer account information.

D. Alerts from Others

Red Flag

1. Notice to the Town from a customer, 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.

IV. DETECTING RED FLAGS.

A. New Accounts

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

Detect

1. 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;
2. Review documentation showing the existence of a business entity.

B. Existing Accounts

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

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, review driver's license or identification card);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Town 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:

Prevent and Mitigate

1. Mark account in the system and continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account or stop service until identity can be verified;
6. Reopen an account with a new account number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify the appropriate law enforcement; and/or
9. Take no action at all, if no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Town accounts, the Town will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected;
4. Keep offices clear of papers containing customer information;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of customer information that are necessary for Town purposes.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Town from Identity Theft. At least annually, the Program Administrator will consider the Town's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Town maintains and changes in the Town's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program are warranted. If warranted, the Program Administrator will update the Program and present the recommended changes to the Town Council. The Town Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with a Program Administrator. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Town 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.

B. Staff Training and Reports

Town staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

C. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Town'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 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.