RESOLUTION NO. 2011-04

A RESOLUTION ADOPTING THE TOWN OF PLAINFIELD IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Town of Plainfield ("Town") is a municipality that provides utility services to residents;

WHEREAS, the Town is a "creditor" as defined in 16 C.F.R. 681.2, which is also Known as the Federal Trade Commission's Red Flags Rule ("Red Flags rule" or "Rule"), due to the Town's provision or maintenance of covered accounts for which consumer payments are made in arrears;

WHEREAS, in its desire to protect its utility customers against identity theft and comply with 16 C.F. R. 681.2, the Town desires to establish reasonable policies and procedures in an Identity Theft Prevention Program ("Program") for the Utility Department, as set forth in Exhibit "A" attached hereto and incorporated by reference herein;

WHEREAS, 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 Town Council has determined that the Program is appropriate for the Town; and

WHEREAS, the Town Council desires to appoint the Clerk-Treasurer to administer and provide oversight to the Program ("Program Administrator").

NOW THEREFORE, the Town Council adopts and approves this Program as described below, and approves the appointment of the Clerk-Treasurer as Program Administrator as of (date).

Adopted this 14th day of March, 2011, by the Town Council of the Town of Plainfield, Indiana.

TOWN COUNCIL OF THE TOWN OF PLAINFIELD, INDIANA

Robin G. Brandgard, President

Bill Kirchoff, Vice President

Kent McPhail

Edmund L. Gaddie, Jr.

Renea S. Whicker

ATTESTED BY:

Wesley R. Bennett, Clerk-Treasurer
Town of Plainfield, Indiana

EXHIBIT "A"

Town of Plainfield Identity Theft Program
For the Utility Billing Department

TOWN OF PLAINFIELD
IDENTITY THEFT PREVENTION PROGRAM
FOR THE UTILITY BILLING DEPARTMENT

I. PURPOSE OF THE PROGRAM

Complying with the Red Flags Rule

Under the Red Flag rules, every financial institution and creditor is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its operation. This Program is adopted to comply with the Red Flags Rule, in order to identity relevant Red Flags (as defined below), to detect Red Flags, to respond appropriately to Red Flags, and to require the Program to be periodically updated.

II. DEFINITIONS

For the purposes of this Program, the following definitions apply:

1. "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.
2. "Covered" Account" means:
    a. Any account the Department offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
    b. Any other account the Department offers or maintains for which thereis a reasonably foreseeable risk to customers or to the safety and soundness of the Department from Identity Theft.
3. "Creditor" has the same meaning as defined in Section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a, and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the Department.
4. "Customer" means a person or business entity that has a Covered Account with the Department.
5. "Department" means the Utility Billing Department of the Town of Plainfield.
6. "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identity 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 or unique electronic identification number

7. "Identity Theft" means faud committed using the Identifying Information of another person.
8. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
9. "Service Provider" means a person or business entity that provides a service directly to the Town relating to or connection with a Covered Account.

III. TYPE OF ACCOUNTS AND ACCESS TO ACCOUNTS

A. Type of Accounts

The Department currently offers and maintains the following type(s) of Covered Accounts:

Utility Service Account

B. Access to Accounts

Customer Account Information may be accessed in the following ways:

In Person
By Phone
By Mail
By Email

IV. IDENTIFICATION OF RED FLAGS

The Department endeavors to identity relevant Red Flags as they relate to possible risk of Identity Theft in connection with the Department's covered Accounts. Inconsistent documents, information or activity encountered when dealing with Customer Accounts and financial transactions may signal Identity Theft. In order to identify relevant Red Flags, the Department shall initially and annually review and consider the types of covered Accounts that it offers and maintains, the methods it provides to open covered Accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft.

The town identifies the following relevant Red Flags at present, which it will consider in detecting Identity Theft.

A. Suspicious Documents

1. Documents provided for identification that appear to be forged or altered;
2. Documents provided for identification on which a person's photograph or physical description is inconsistent with the person presenting the document;
3. Other document with information that is not consistent with existing Customer information (for example, a person's signature on a check appears forged);
4. Application for services or Account setup that appears to have been altered or forged; and
5. Social Security Numbers that are always invalid:
   The first three digits are in the 772-800 or the 900 range;
   The first three digits are 666; or
   The first three digits are 000, or the fourth and fifth digits are 00, or the last four digits are 0000.

B. Suspicious Personal Identifying Information

1. Identifying Information presented that is inconsistent with other information the Customer provides, or information that is on file for that Customer (such as 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 driver's license, or signatures that do not appear to match other documents);
3. Identifying Information presented that is the same as information that is included on applications that are known to be fraudulent (such as a name or Social Security number that has been identified as being fraudulent on other prior applications received for various applicants);
4. Identifying Information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Identifying Information presented, such as a Social Security number, phone number, or address that is the same as one given by another Customer; and
6. Failing to provide complete personal Identifying Information on an application when reminded to do so.

C. Unusual Use or Suspicious Activity of Covered Account

1. Change of billing address for an Account followed by a request to change the Account holder's name or add other authorized user(s) on the Account:

2. Payments stop on an otherwise consistently up-to-date Account;
3. Account used in a way that is not consistent with prior use (such as very high activity);
4. Change of payment method where payment is charged to an individual not listed on the Account/
5. Mail sent to the Account holder is repeatedly returned as undeliverable;
6. Notice to the Department that a Customer is not receiving mail sent by the Department;
7. Notice to the Department that an Account has unauthorized activity;
8. Breach in the Department computer system security; and
9. Unauthorized access to or use of Customer Account information.

D. Alerts from Others or Past History in Incidents of Identity Theft

1. Notice to the Department from a Customer, a victim of Identity Theft, a law enforcement authority or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft;
2. Checks returned for insufficient funds or credit card payments or EFTs that are declined, especially when a pattern is noticed or following a change in method of payment; and
3. Past experiences the Department has had regarding incidents of Identity Theft, when similar patterns or events are noticed by the Town.

V. DETECTING RED FLAGS

The Department hereby establishes the following procedures to assist in detecting Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts.

A. New Accounts

New Accounts may be opened in person, by fax or by mail or phone. In all cases, a potential Customer must submit All of the following information:

Full legal name
Telephone Number
Mailing Address
Social Security Number
Must be on the lease if a rental property

B. Existing Accounts

When handling a transaction regarding an existing Account, the Department staff will take the following steps to monitor transactions with an Account in order to detect possible Red Flags as listed above:

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

VI. RESPONDING TO RED FLAGS

In the event a Town employee detects any identified Red Flags, the employee shall respond by taking one or more of the following steps to investigate, prevent and mitigate possible Identity Theft, depending on the degree of risk posed by the Red Flag:

A. Investigate, Prevent and Mitigate Identity Theft

Upon detecting a Red Flag, employees must take the following action:

1. Gather relevant documentation regarding the suspect Covered Account;
2. Report the identified Red Flag to the Program Administrator;
3. Contact the Customer with the Covered Account; and
4. Assist Program Administrator in investigating the Red Flag issue.

After receiving a Red Flag report, the Program Administrator may take one or more of the following actions as warranted under the particular circumstances in the discretion of the Program Administrator:

1. Monitor a Covered Account for evidence of Identity Theft;
2. Change any passwords or other security codes and devices that permit access to a Covered Account;
3. Close the existing Covered Account;
4. Open a new Covered Account with a new number;
5. Put a hold on attempting to collect payment on a Covered Account; and/or
6. Notify the Plainfield Police Department.

B. Ongoing Protection of Customer Identifying Information

The Department shall take the following steps with respect to its internal operating procedures in order to take an active role in the ongoing protection of Customer Identifying Information from Identity Theft:

1. Paper documents

a. Storage. Documents containing Customer Identifying Information must be stored in locked file cabinets contained within a locked room except when an employee is working on the file. Only specially identified employees with a legitimate need shall have keys or swipe card to the file cabinets and storage room.

b. Use of Documents. Department employees must not leave documents containing Customer Identifying Information out on their desks when they are away from their workstations. Department employees must store documents containing Customer Identifying Information in Locked areas when leaving their work areas.

2. Computers and Electronic Media

a. Passwords. All computers must be set to require passwords. Each employee must have a unique username and password, which must be different from each other, and shall not be posted at his or her workstation. When new software is installed, the default passwords must be changed. Department employees must log off their computers when leaving their workstations, and computer screens must be set to lock after a set period of time.

b. Firewalls and Anti-Virus. The Town's website and network systems must be secured with adequate firewalls and regularly updated anti-virus and anti-theft software. Anti-virus and anti-spyware programs must be run on the server daily. The Town's website must provide clear notice to Customers that the website is not a "secure" website.

3. Destruction of Documents and Other Media

a. Paper records. All paper records containing Customer Identifying Information that are designated for disposal must be shredded before being placed into a trash bin. A paper shredder or shredding bin provided by a shredding company must be located in each department containing Customer Identifying Information.

b. Other media. Any other data storage media containing Customer Identifying Information that are designated for disposal must be destroyed by shredding, hole punching or incineration.

4. Visitors and Access

a. Access. Department employees must lock office doors when leaving their work areas. Access to any offsite facilities is limited to Department employees with a legitimate business need.

b. Visitors. Visitors who enter any area where records containing Customer Identifying Information are kept must be escorted by an authorized Department employee. No visitor shall be given any entry code, key, or swipe card, or allowed unescorted access to any such area.

5. Employment Practices

a. New Hires. Before hiring any new employee who will have access to Customer Identifying Information, the Human Resource Department must first complete a reference and background check of such potential employee. All employees must also sign an agreement to follow the Town's confidentiality and security standards for handling Customer Identifying Information.

b. Exit Requirements. If an employee leaves the Department's employ or is reassigned duties that no longer require access to Customer Identifying Information, the employee must return all keys and swipe cards to the Program Administrator. Immediately upon the employee's departure or reassignment, the Program Administrator shall ensure that all of such employee's passwords allowing access to Customer Identifying Information are changed.

c. Policy Violations. Any employee who violates this Identity Theft Prevention Program and any security policy or procedure adopted hereunder will be subject to immediate discipline, which may include dismissal.

VII. PROGRAM EVALUATION AND REVISIONS

The Program Administrator, and the Town Council will at least annually evaluate and revise the Program to reflect changes in risks to Covered Accounts and to the safety and soundness of the Town from Identity Theft. The annual Program review and evaluation process shall consider the Town's experiences with Identity Theft, changes in Identity Theft detection and prevention methods, changes in types of Account that the

Town maintains and changes in the Town's business arrangements with other entities and Service Providers. Following the review and consideration of those factors, the Program Administrator shall revise the program as necessary. If warranted, the Program Administrator shall update and implement the revised Program and obtain Town Council approval of such changes.

VIII. ADMINISTRATION AND OVERSIGHT OF THE PROGRAM

A. Oversight

The Program Administrator shall be responsible for the Program administration, for staff training on the Program as appropriate, for reviewing any reports regarding the detection of Red Flags, for determining and instituting the necessary steps to prevent and mitigate Identity Theft when Red Flags are detected, and for periodically reviewing and revising the Program. The Program Administrator shall maintain, for a reasonable amount of time and as appropriate and necessary, reports and documentation regarding incidents of detected Red Flags.

B. Staff Training and Reports

The Town employees that are responsible for implementing the Program shall be trained wither by or under the direction of the Program Administrator in the detection of Red Flags, and the steps to be taken in responding to Red Flags. Such staff shall be trained on how to report detected Red Flags.

C. Service Provider Arrangements

In the event the Town engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the Town shall take the following steps to require that the Service Provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

1. Require, by contract, that Service Provider acknowledges receipt and review of the Program and agrees to perform its activities with respect to the Town's Covered Accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program; or

2. Require, by contract, that Service Provider acknowledges receipt and review of the Program and agrees to perform its activities with respect to the Town's Covered Accounts in compliance with the terms and conditions of the Service Provider's Identity Theft prevention program and will take appropriate action to prevent and mitigate Identity Theft; and that the Service Provider agrees to report promptly to the Town in writing if the Service Provider in connection with a Town Covered Account detects an incident of actual or attempted Identity Theft

or is unable to resolve one or more Red Flags that the Service Provider detects in connection with a Covered Account.

D. Customer Identifying Information and Public Disclosure

The Identifying Information of the Department's Customers with Covered Accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law, including, Indiana Code 5-14-3-4. The Town Council also finds and determines that public disclosure of the Town's specific practices to identity, detect, prevent and mitigate Identity Theft may compromise the effectiveness of such practices and hereby directs that, under the Program, knowledge of such specific practices shall be limited to the Program Administrator and those Town employees and Service Providers who need to be aware of such practices for the purpose of preventing Identity Theft.