ORDINANCE NUMBER 644

AN ORDINANCE ESTABLISHING THE TOWN OF YORKTOWN IDENTITY THEFT PREVENTION PROGRAM

---

WHEREAS, the Federal Trade Commission, through 16 C.F.R. Part 681.1, adopted Identity Theft Rules requiring financial institutions and creditors that offer or maintain one or more covered accounts to develop and provide for the continued administration of a written program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account; and,

WHEREAS, the Town of Yorktown provides municipal utilities in the form of water and sewage services and the Federal Trade Commission regulations mandate compliance by utility companies; and,

WHEREAS, the Federal Trade Commission has recognized that in designing its program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft; and,

WHEREAS, this document contains the written identity theft prevention program for the Town of Yorktown, Indiana in accordance with the regulations of the Federal Trade Commission at 16 C.F.R. Part 681., and this Program shall be adopted, implemented, maintained, administered, updated, and interpreted so as to be consistent and in accordance and compliance with the requirements of these regulations; and,

WHEREAS, this Program is appropriate to the size and complexity of the Town and the nature and scope of its activities.

NOW, THEREFORE, BE IT ORDAINED by the Town Council of the Town of Yorktown, Indiana, as follows:

## Section 1. Short Title

This policy shall be known as the Town of Yorktown Identity Theft Prevention Program ("Program").

## Section 2. Purpose

The purpose of this Program is to comply with the Federal Trade Commission's Fair Credit Reporting Act, specifically the Identity Theft Rules and federal regulations promulgated at 16 C.F.R. Part 681 aimed at detecting, preventing, and mitigating identity theft by recognizing Red Flags in connection with the opening of a Covered Account or any existing Covered Account.

## Section 3. Definitions

For purposes of this Program, the following definitions apply:

a. "Account" means a continuing relationship established by a Person with the Town to obtain a product or service for personal, family, household, or business purposes. Account includes:
    i. An extension of credit, such as the purpose of property or services involving a deferred payment; and,
    ii. A deposit account.
b. "Covered Account" means:
    i. Any account that the Town offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and
    ii. Any other account the Town offers or maintains for which there is a reasonably foreseeable risk to the account holder or to the safety and soundness of the Town from identity theft, including financial, operational, compliance, reputation, or litigation risks.
c. "Credit" means the right granted by a Creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
d. "Creditor" means:
    i. Any Person who regularly extends, renews, or continues credit;
    ii. Any Person who regularly arranges for the extension, renewal, or continuation of credit; or,
    iii. Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

    "Creditor" includes utility companies and telecommunications companies.
e. "Customer" means a person that has a Covered Account with the Town.
f. "Identity Theft" means a fraud committed or attempted using identifying information of another Person without authority.
g. "Person" means a natural person, corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
h. "Program" means this Town of Yorktown Identity Theft Prevention Program.
i. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
j. "Service Provider" means a Person that provides a service directly to the Town.
k. "Town" means the Town of Yorktown, Indiana.
l. "Utility Department" means the Town of Yorktown Utility Department.

## Section 4. Findings

As of the date of this Program, the Town makes the following findings:

a. The Town is a Creditor due to its provision for and maintenance of Covered Accounts for which payment is made in arrears.
b. The Town provides the following types of Covered Accounts:
    i. Water Utility Accounts;
    ii. Sewer Utility Accounts;
    iii. Trash Utility Accounts;
c. The potential processes in which Identity Theft could occur include:
    i. Opening a new Covered Account;
    ii. Restoring an existing Covered Account;
    iii. Making payments on Covered Accounts;
    iv. Providing account information and access in person or via the telephone or world wide web

## Section 5. Aspects of the Program

This Program shall include reasonable policies and procedures to:

a. Identify relevant Red Flags and incorporate them into this Program;
b. Detect Red Flags that have been incorporated into this Program;
c. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
d. Ensure that the Program is updated periodically to reflect changes and risks to the Town's Customers and to the safety and soundness of the Town.

## Section 6. Identifying Red Flags

The Red Flags listed in Exhibit A include, but are not limited to, the Red Flags that are most applicable to the Town and its Covered Accounts. The following Red Flag categories are applicable to this Program:

a. Alerts, notifications, or warnings from a consumer reporting agency;
b. Suspicious documents;
c. Suspicious personal identifying information;
d. Unusual use of, or suspicious activity related to, the Covered Account; and,
e. Notice from Customers, victims of Identity Theft, or other persons.

## Section 7. Detecting Red Flags

Under this Program:

a. All employees responsible for or involved in the process of opening a Covered Account, restoring a Covered Account, or accepting payment for a Covered Account shall check for Red Flags as indicators of possible Identity Theft.
b. In order to facilitate detection of the Red Flags identified in Section 6 and Exhibit A of this policy, appropriate staff will take the following steps to verify:
    i. The identity of a Person opening a new Covered Account (e.g. driver's license, government issued ID, or multiple pieces of other identification); and,
    ii. The validity of requests for changes of billing address and verifying identification of Customers before giving out any personal information for existing Covered Accounts.

## Section 8. Response to Red Flag Detection

Any employee that may suspect fraud or Identity Theft or detect a Red Flag will implement the following response(s) as applicable:

a. All suspicious activity and detections of Red Flags shall be reported to the Utility Department Billing Office.
b. Additional response(s) may include, but are not limited to:
    i. Asking the applicant for clarification or additional documentation.
    ii. Notifying the Yorktown Police Department.
    iii. Declining to open the Account.
    iv. Monitoring the Account.
    v. Closing the Account.
    vi. Contacting the Customer.
    vii. Not attempting to collect on an Account.
    viii. Determining that no response is warranted under the particular circumstances when the detected Red Flag is resolved.

## Section 9. Other/Additional Accounts

In the event the Town or Utility Department staff detects Red Flags with respect to any other Accounts of the Town, an appropriate response to such Red Flags shall be implemented in accordance with this Program.

## Section 10. Updating the Program

This Program shall be reviewed at least annually and updated when necessary to reflect changes and risks to Customers and to the safety and soundness of the Town. Upon review, consideration will be given to:

a. The experiences of the Utility Department and Town with Identity Theft;
b. Changes in methods of Identity Theft;

c. Changes in methods to detect, prevent, and mitigate Identity Theft, including additional relevant Red Flags;
d. Changes in the types of Covered Accounts the Town offers or maintains; and,
e. Changes in the business arrangements of the Town including Service Provider arrangements.

## Section 11. Program Administration

This Program shall be administered in the following manner:

a. This Program shall be initially approved by the Town Council of the Town of Yorktown, Indiana.
b. The Utility Department shall be designated responsible for the oversight, development, implementation, and administration of the Program. The Utility Department shall annually report to the Town Council regarding compliance by the Town with the Red Flag regulations found in 16 C.F.R. Part 861.
c. The Utility Department shall train staff, as necessary, to effectively implement this Program.
d. Legal counsel for the Town may be contacted as necessary with respect to the requirements of this Program.
e. When the Town engages a Service Provider to perform an activity in connection with Covered Accounts, the Town should take steps to ensure that the activity of the Service Provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

ADOPTED AND APPROVED by the Town Council of the Town of Yorktown, Indiana this _____day of _____, 2009.

TOWN COUNCIL OF THE TOWN OF YORKTOWN, INDIANA

_____ _____

Steve Lowry, President Rick Glaub, Vice President

_____ _____

Mike Beeman, Member Bob Flanagan, Member

_____

Larry Crouch, Member

ATTEST:

_____

Beth Neff, Clerk-Treasurer

## EXHIBIT A

---

## RED FLAGS

The following are illustrative examples of Red Flags in connection with Covered Accounts:

Alerts, Notifications, Warnings, from a Consumer Reporting Agency

Any alert, notification, warning, or inquiry from a consumer reporting agency concerning any fraud, possible fraud, identity theft, or potential identity theft involving a customer.

Suspicious Documents

a. Documents provided for identification that appear to have been altered or forged.
b. A photograph or physical description on any identification is not consistent with the appearance of the applicant or customer presenting the identification.
c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
d. Other information on the identification is not consistent with readily accessible information that is on file with the Town, such as a signature card or a recent check.
e. Any information provided that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

a. Personal identifying information provided is inconsistent when compared against external information sources used by the Town. For example:
    i. The address does not match any address in the consumer reports; or
    ii. The Social Security Number ("SSN") has not been issued, or is listed on the Social Security Administration's Death Master File.
b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided. For example, there is a lack of correlation between the SSN range and date of birth.
c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Town. For example:

i. The address on an application is the same as the address provided on a fraudulent application; or
ii. The phone number on an application is the same as the number provided on a fraudulent application.

d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Town. For example:

i. The address on an application is fictitious, a mail drop, or a prison; or
ii. The phone number is invalid, or is associated with a pager or answering service.

e. The SSN provided is the same of that provided by other persons opening an account or other customers.
f. The address or telephone number provided is the same as the address or telephone number submitted by other persons opening accounts or other customers.
g. The person opening the account or the customer fails to provide all requested personal identifying information.
h. Personal identifying information provided is not consistent with personal identifying information on file with the Town.

Unusual Use of, or Suspicious Activity Related to, the Account

a. An account is used in a manner that is not consistent with established patterns of activity on the account.

b. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.

c. The Town is notified that the customer is not receiving paper account statements.

d. The Town is notified of unauthorized charges or transactions in connection with the customer's account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft

The Town is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.