

ORDINANCE 1424

**AN ORDINANCE ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM  
TO BE IN COMPLIANCE WITH THE FEDERAL TRADE COMMISSION'S  
RED FLAG RULE**

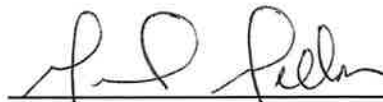
**WHEREAS**, The Town of Munster Water Utility, Lake County, Indiana, is a municipal water utility; and,

**WHEREAS**, The Federal Trade Commission, in conjunction with other federal agencies, has required all United States utilities to develop and implement an identity theft prevention program; now, therefore, be it

**ORDAINED**, By the Munster Town Council, acting as the Town of Munster Water Utility, Lake County, Indiana, that the attached Exhibit A be adopted as the Identity Theft Prevention Program as required by the Red Flag rule of the Federal Trade Commission.

**ADOPTED AND PASSED** this 6<sup>TH</sup> day of APRIL 2009, by a vote of 4 in favor and 0 opposed.

TOWN COUNCIL OF THE  
TOWN OF MUNSTER,  
LAKE COUNTY, INDIANA



Michael Mellon, President

ATTEST:

  
David F. Shafer, Clerk-Treasurer

## ORDINANCE 1424, EXHIBIT A

---

Identity Theft Prevention Program  
for  
Town of Munster Water Utility  
1005 Ridge Road  
Munster, Indiana 46321  
March 9, 2009

---

### **Town of Munster Water Utility Identity Theft Prevention Program**

This Plan is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, provide methods to ensure existing accounts were not opened using false information, and recite measures to respond to such events.

#### Contact Information:

The Senior Management Person responsible for this plan is:

Name: Thomas F. DeGiulio

Title: Town Manager

Phone number: 219-836-6900

The Governing Body Members of the Utility are:

Board Members

1. Michael Mellon
  2. Helen Brown
  3. John Edington
  4. Robert Mangus
  5. David Nellans
-

## **Risk Assessment**

The Town of Munster Water Utility has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the utility was able to identify red flags that were appropriate to prevent identity theft:

- ☐ New accounts opened In Person
  - ☐ New accounts opened via Telephone
  - ☐ New accounts opened via Fax
  - ☐ New accounts opened via Web
  - ☐ Account information accessed In Person
  - ☐ Account information accessed via Telephone (Person)
  - ☐ Account information is accessed via Telephone (Automated)
  - ☐ Account information is accessed via Web Site
  - ☐ Identity theft occurred in the past from someone falsely opening a utility account
- 

## **Detection (Red Flags):**

The Town of Munster adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary:

- ☐ Fraud or active duty alerts included with consumer reports
- ☐ Notice of credit freeze provided by consumer reporting agency
- ☐ Notice of address discrepancy provided by consumer reporting agency
- ☐ Inconsistent activity patterns indicated by consumer report such as:
  - ☐ Recent and significant increase in volume of inquiries
  - ☐ Unusual number of recent credit applications
  - ☐ A material change in use of credit
  - ☐ Accounts closed for cause or abuse
- ☐ Identification documents appear to be altered
- ☐ Photo and physical description do not match appearance of applicant
- ☐ Other information is inconsistent with information provided by applicant
- ☐ Other information provided by applicant is inconsistent with information on file.
- ☐ Application appears altered or destroyed and reassembled

- ❑ Personal information provided by applicant does not match other sources of information (e.g., credit reports, social security number not issued or listed as deceased)
  - ❑ Lack of correlation between the social security number range and date of birth
  - ❑ Information provided is associated with known fraudulent activity (e.g., address or telephone number provided is same as that of a fraudulent application)
  - ❑ Information commonly associated with fraudulent activity is provided by applicant (e.g., address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
  - ❑ Social security number, address, or telephone number is the same as that of other customer at utility
  - ❑ Customer fails to provide all information requested
  - ❑ Personal information provided is inconsistent with information on file for a customer
  - ❑ Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
  - ❑ Identity theft is reported or discovered
- 

## **Response**

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the senior management official.

- ❑ Ask applicant for additional documentation
  - ❑ Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Clerk-Treasurer or Accounting Supervisor
  - ❑ Notify law enforcement: The utility will notify The Munster Police Department at 219-836-6600 of any attempted or actual identity theft.
  - ❑ Do not open the account
  - ❑ Close the account
  - ❑ Do not attempt to collect against the account but notify authorities
-

## **Personal Information Security Procedures:**

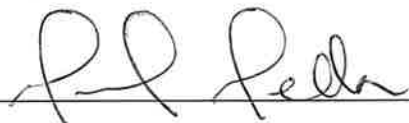



The Town of Munster Water Utility adopts the following security procedures.

1. Paper documents, files and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.
  2. Access to offsite storage facilities is limited to employees with a legitimate business need.
  3. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the Utility.
  4. When sensitive data is received or transmitted, secure connections will be used.
-

## Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the Utility Board of Directors. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Signatures:

1.		Date _____
2.		Date <u>4-6-09</u>
3.		Date <u>4-6-09</u>
4.		Date <u>4-6-09</u>
5.	_____	Date _____

A report will be prepared annually and submitted to the above named senior management or governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third-party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.