ORDINANCE 1514

AN ORDINANCE AMENDING ORDINANCE 1424 REGARDING THE IDENTITY THEFT PREVENTION PROGRAM (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;

WHEREAS, The membership of the Water Utility Board has changed; now, therefore, be it

ORDAINED, By 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 with current Water Utility Board information.

ADOPTED AND PASSED this 14TH day of MARCH 2011, by a vote of 5 in favor and 0 opposed.

TOWN COUNCIL OF THE TOWN OF MUNSTER, LAKE COUNTY INDIANA

Robert H. Mangus, President

ATTEST:

David F. Shafer, Clerk-Treasurer

EXHIBIT A

Identity Theft Prevention Program
For
Town of Munster Water Utility
1005 Ridge Road
Munster, Indiana 46321
March 9, 2009 (original adoption)
March 14, 2011 (1st revision)

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, methods to ensure existing accounts were not opened using false information, and 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. John Edington
2. Andy Koultourides
3. Robert Mangus
4. Michael Mellon
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, SS# not issued or listed as deceased)
- ❑ Lack of correlation between the SS# range and date of birth
- ❑ Information provided is associated with known fraudulent activity (e.g. address or phone 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)
- ❑ SS#, address, or telephone # 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 (select appropriate procedures from Appendix A and add other procedures as appropriate).

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 date 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 3/14/11

2. _____ Date 3-14-11

3. _____ Date 3/14/11

4. _____ Date 3/14/11

5. _____ Date 3/14/11

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.

Appendix A

Other Security Procedures

The following suggestions are not part of or required by the Federal Trade Commission's "Identity Theft Red Flags Rule". The following is a list of other security procedures a utility should consider to protect consumer information and to prevent unauthorized access. Implementation of selected actions below according to the unique circumstances of utilities is a good management practice to protect personal consumer data.

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. Only specially identified employees with a legitimate need will have keys to the room and cabinet.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees will not to leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas
6. Employees log off their computers when leaving their work areas
7. Employees lock file cabinets when leaving their work areas
8. Employees lock file room doors when leaving their work areas
9. Access to offsite storage facilities is limited to employees with a legitimate business need.
10. Any sensitive information shipped using outside carriers or contractors will be encrypted
11. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery this information.
12. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.

13. No visitor will be given any entry codes or allowed unescorted access the office.

14. Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.

15. Passwords will not be shared or posted near workstations.

16. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

17. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

18. Sensitive consumer data will not be stored on any computer with an Internet connection

19. Sensitive information that is sent to third parties over public networks will be encrypted

20. Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.

21. Email transmissions within your business will be encrypted if they contain personally identifying information.

22. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.

23. When sensitive data is received or transmitted, secure connections will be used

24. Computer passwords will be required.

25. User names and passwords will be different.

26. Passwords will be changed at least monthly.

27. When installing new software, vendor-supplied default passwords are changed.

28. The use of laptops is restricted to those employees who need them to perform their jobs.

29. Laptops are stored in secure place.

30. Laptop users will not store sensitive information on their laptops.

31. Laptops which contain sensitive data will be encrypted

32. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.

33. If a laptop must be left in a vehicle, it is locked in a trunk.

34. The computer network will have a firewall where your network connects to the Internet.

35. Any wireless network in use is secured.

36. Maintain central log files of security-related information to monitor activity on your network.

37. Monitor incoming traffic for signs of a data breach.

38. Monitor outgoing traffic for signs of a data breach.

39. Implement a breach response plan.

40. Check references or do background checks before hiring employees who will have access to sensitive data.

41. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.

42. Access to customer's personal identify information is limited to employees with a "need to know."

43. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.

44. Implement a regular schedule of employee training.

45. Employees will be alert to attempts at phone phishing.

46. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.

47. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

48. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

49. Paper records will be shredded before being placed into the trash.

50. Paper shredders will be available at each desk in the office, next to the photocopier, and at the home of any employee doing work at home.

51. Any data storage media will be disposed of by shredding, punching holes in, or incineration.