

ORDINANCE NO. 041409

AN ORDINANCE ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, pursuant to Federal law, the Federal Trade Commission adopted Identity Theft Rules, known as the Identity Theft Prevention Program (hereinafter called the “Program”) requiring the creation of certain policies relating to the use of consumer reports, addresses discrepancy and the detection, prevention and mitigation of identity theft; and,

WHEREAS, the Federal Trade Commission regulations, adopted as 16 CFR § 1681a (r)(5) to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts; and,

WHEREAS, the Program specifically includes utility companies, including municipal utilities to comply, and;

WHEREAS, the Town of McCordsville provides Sewer and Stormwater Utility Services.

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

SECTION I. Short Title.

This policy shall be known as the Identity Theft Prevention Program (hereinafter “Program”).

SECTION II. Purpose.

This policy is adopted to comply with the Fair and Accurate Credit Transactions Act and federal regulations promulgated at 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

SECTION III. Definitions.

For purposes of this policy, the following definitions apply:

1. ‘Covered account’ means (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a

credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2. '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.
3. 'Creditor' means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.
4. 'Customer' means a person that has a covered account with a creditor.
5. 'Identity theft' means a fraud committed or attempted using identifying information of another person without authority.
6. 'Notice of address discrepancy' means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.
7. 'Person' means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
8. 'Personal Identifying Information' means a person's credit card account information, debit card information bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.
9. 'Red flag' means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
10. 'Service provider' means a person that provides a service directly to the city.

SECTION IV. Findings.

1. The Town of McCordsville Utility Department (known hereafter as the Utility Department) is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.
2. Covered accounts offered to customers for the provision of services include Sewer Utility and Stormwater Utility.
3. The Utility Department's previous experience with identity theft related to covered accounts is as follows: No known incidents.
4. The processes of opening a new covered account, restoring an existing covered account, making payments on such accounts, and providing account information, access in person or via phone or website have been identified as potential processes in which identity theft could occur.
5. The Utility Department limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered directly into the Utility Department's computer system and is not otherwise recorded.
6. The Utility Department determines that there is a low risk of identity theft occurring in the following ways (*if any*):
 - a. Use by an applicant of another person's personal identifying information to establish a new covered account;
 - b. Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name;
 - c. Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts;
 - d. Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account, or other method of payment.

SECTION V. Process of Establishing a Covered Account.

As a precondition to opening a covered account, each applicant shall provide name, address, telephone number, owner of property and occupancy date with personal identifying information of the customer. Such information shall be entered directly into the Utility Department's computer system and shall not otherwise be recorded. Each account shall be assigned an account number and personal identification number (PIN)

which shall be unique to that account. The Utility Department may utilize computer software to randomly generate assigned PINs and to encrypt account numbers and PINs.

SECTION VI. Access to Covered Account Information.

1. Access to customer accounts shall be password protected and shall be limited to authorized personnel.
2. Such password(s) shall be changed on a regular basis by each individual user, shall be at least 8 characters in length, and shall contain letters, numbers and symbols.
3. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Utility Billing Supervisor and the password changed immediately.
4. Personal identifying information included in customer accounts is considered confidential, **(to the extent allowed by law)** and any request or demand for such information shall be immediately forwarded to the Utility Billing Supervisor.

SECTION VII. Credit Card Payments.

1. In the event that credit card payments that are made over the Internet are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.
2. All credit card payments made over the telephone or the Town of McCordsville's website shall be entered directly into the customer's account information in the computer data base.
3. Account statements and receipts for covered accounts shall include only the last four digits of the credit or debit card or the bank account used for payment of the covered account.

Section VIII. Sources and Types of Red Flags.

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. Such red flags shall include, but not be limited to:

1. Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of such alerts are:

- a. A fraud or active duty alert that is included with a consumer report
 - b. A notice of credit freeze in response to a request for a consumer report
 - c. A notice of address discrepancy discovered through the Hancock County Geographic Information System
2. Suspicious documents. Examples of suspicious documents include:
- a. Documents provided for identification that appear to be altered or forged
 - b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer
 - c. Identification on which the information is inconsistent with information provided by the applicant or customer
 - d. Identification on which the information is inconsistent with readily accessible information that is on file, such as a signature card or a recent check or
 - e. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.
3. Suspicious personal identifying information. Examples include:
- a. Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:
 - (i) The address does not match any address in the consumer report; or
 - b. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the financial institution or creditor.
 - c. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
 - d. The SSN provided is the same as that submitted by other applicants or customers.
 - e. The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of applicants or customers.
 - f. The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - g. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.
 - h. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
4. Unusual use of or suspicious activity relating to a covered account. Examples include:

- a. Shortly following the notice of a change of address for an account, there is a request for the addition of authorized users on the account.
 - b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns, such as where the customer fails to make the first payment or makes an initial payment but no subsequent payments.
 - c. An account is used in a manner that is not consistent with established patterns of activity on the account, such as:
 - (i) Nonpayment when there is no history of late or missed payments
 - d. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
 - e. The Utility Department is notified that the customer is not receiving paper account statements.
 - f. The Utility Department is notified of unauthorized charges or transactions in connection with a customer's account.
 - g. The Utility Department is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.
5. Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts

SECTION IX. Prevention and Mitigation of Identity Theft.

1. In the event that any employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the McCordsville Police Department. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Utility Billing Supervisor, who may in his or her discretion determine that no further action is necessary. If the Utility Billing Supervisor in his or her discretion determines that further action is necessary, one or more of the following responses as determined to be appropriate by the Utility Billing Supervisor shall be performed:
 - a. Contact the customer;
 - b. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the

customer's covered account:

- (i) change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
 - (ii) close the account;
 - c. Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;
 - d. Notify law enforcement in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or
 - e. Take other appropriate action to prevent or mitigate identity theft.
2. In the event that an employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect to an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the McCordsville Police Department. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Utility Billing Supervisor, who may in his or her discretion determine that no further action is necessary. If the Utility Billing Supervisor in his or her discretion determines that further action is necessary, one or more of the following responses as determined to be appropriate by the Utility Billing Supervisor shall be performed:
- a. Request additional identifying information from the applicant;
 - b. Deny the application for the new account;
 - c. Notify law enforcement of possible identity theft; or
 - d. Take other appropriate action to prevent or mitigate identity theft.

SECTION X. Updating the Program.

The Utility Department shall annually review and, as deemed necessary, update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the Utility Department and its covered accounts from identity theft. In so doing, the Utility Department shall consider the following factors and exercise its discretion in amending the program:

- 1. The Utility Department experiences with identity theft;
- 2. Updates in methods of identity theft;
- 3. Updates in customary methods used to detect, prevent, and mitigate identity theft;

4. Updates in the types of accounts that the Utility Department offers or maintains; and
5. Updates in service provider arrangements.

SECTION XI. Program Administration.

The Utility Billing Supervisor is responsible for oversight of the program and for program implementation. The Utility Billing Supervisor is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the Utility Billing Supervisor, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program shall be submitted to Town Manager.

The Utility Billing Supervisor will report to Town Manager at least annually on compliance with the red flag requirements. The report shall be due no later than December 31st each year and shall address material matters related to the program and evaluate issues, including but not limited to:

1. The effectiveness of the program policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
2. Service provider arrangements;
3. Significant incidents involving identity theft and management's response; and
4. Recommendations for material changes to the Program.

The Utility Billing Supervisor is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The Utility Billing Supervisor shall exercise his or her discretion in determining the amount and substance of training necessary.

SECTION XII. Outside Service Providers.

In the event that the Utility Department engages a service provider to perform an activity in connection with one or more covered accounts the Utility Billing Supervisor shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft."

SECTION XIII. Treatment of Address Discrepancies.

In the event that the Utility Department receives a notice of address discrepancy, the employee responsible for verifying consumer addresses for the purpose of providing the service or account sought by the consumer shall perform one or more of the following activities, as determined to be appropriate by such employee:

1. Compare the information in the consumer report with:
 - a. Information the Utility Department obtains and uses to verify a consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 31 U.S.C. § 5318(l);
 - b. Information the Utility Department maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or
 - c. Information the Utility Department obtains from third-party sources that are deemed reliable by the relevant employee; or
 - d. Verify the information in the consumer report with the consumer.

SECTION XIV. Methods of Confirming Consumer Addresses.

The employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

1. Verifying the address with the consumer;
2. Reviewing the Utility Department records to verify the consumer's address;
3. Verifying the address through third party sources; or
4. Using other reasonable processes.

SECTION XV.

This Ordinance shall be in full force and effect from and after its passage and publication as prescribed by law.

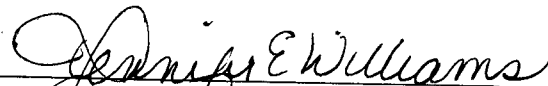
SECTION XVI.


Introduced and filed on the 14th day of April, 2009. A motion to consider on first reading on the day of introduction was offered and sustained by a vote of 5 in favor and 0 opposed pursuant to I.C. 36-5-2-9.8.

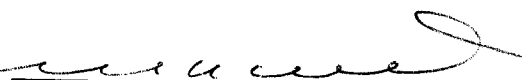
Duly ordained and passed this 14th day of April, 2009 by the Town Council of the Town of McCordsville, Hancock County, Indiana, having been passed by a vote of 5 in favor and 0 opposed.

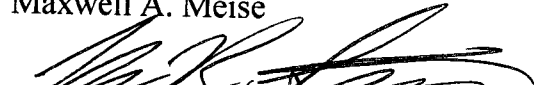
TOWN OF MCCORDSVILLE, INDIANA, BY ITS TOWN COUNCIL


Voting Affirmative:


Jennifer E. Williams



Brent Barnes


Maxwell A. Meise


Thomas R. Strayer


Barry Wood

ATTEST:


Catherine C. Gardner
Clerk-Treasurer

Voting Opposed:

Jennifer E. Williams

Brent Barnes

Maxwell A. Meise

Thomas R. Strayer

Barry Wood

This instrument was prepared by Gregg H. Morelock, BRAND DAVIS & MORELOCK, P.O. Box 6, 6 West South Street, Greenfield, IN 46140.

I affirm, under the penalties for perjury, that I have taken reasonable care to redact each Social Security number in this document, unless required by law. Gregg H. Morelock.