ORDINANCE ESTABLISHING IDENTITY THEFT PREVENTION PROGRAM

ORDINANCE 2009-5

WHEREAS, pursuant to the Federal Trade Commission adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancy and the detection, prevention and mitigation of identity theft;

WHEREAS, the Federal Trade Commission regulations require creditors to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts;

WHEREAS, the Federal Trade Commission's regulations include utility provides in the definition of "creditor";

WHEREAS, the Town of Redkey, Indiana, is a "creditor" by virtue of providing utility services;

WHEREAS, the Federal Trade Commission regulations define "covered account" in part as an account that a creditor provides for personal, family, or household purposes that is designed to allow multiple payments or transactions and specifies that a utility account is a covered account;

WHEREAS, the Federal Trade Commission regulations require each creditor to adopt an Identity Theft Prevention Program which will use red flags to detect, prevent, and mitigate identity theft related to information used in covered accounts; and

WHEREAS, the Town of Redkey, Indiana, provides sanitary sewer, storm water and water utility services for which payment is made after the product is consumed or the service has otherwise been provided which by virtue of being utility accounts are covered accounts.

NOW BE IT ORDAINED BY THE TOWN COUNCIL OF THE TOWN OF REDKEY, INDIANA:

Section 1. Short Title
This policy shall be known as the Identity Theft Prevention Program (hereinafter "Program").

Section 2. Purpose.

This policy is adopted to comply with 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 thet will prevent identity theft.

Section 3. Definitions.
For purposes of this policy, the following definitions apply:

(a) '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 accoun, morgage 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 i 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.

(b) 'Credit' means the right granted by a creditor to a debtor to defer payments of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

(c) '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.

(d) 'Customer' means a person that has a covered account with a creditor.

(e) 'Identity theft' means a fraud committed or attempted using identifying information of another person without authority.

(f) '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.

(g) 'Person' means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(h) 'Personal Identifying Information' means a person's credit card

account , information, debit card information bank account information and driver's license information and for a natural person includes their social security number, mother's birth name, and date of birth.

(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 city.

Section 4. Findings.

(1) The Town of Redkey, Indiana 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 sanitary sewer, storm water and water utility services.

(3) The processes of opening a new covered account, restoring an existing covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur.

(4) The Town of Redkey 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 Town of Redkey's computer system and is not otherwise recorded .

(5) The Town of Redkey determines that there is a low risk of identify theft occurring in the following ways:

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 5. Process of Establishing a Covered Account.

(1) As a precondition to opening a covered account, each applicant shall provide the Town of Redkey with personal identifying information of the customer a valid government issued identification card containing a photograph of the customer or, for customers who are not natural

persons, a photograph of the customer's agent opening the account. Such information shall be entered directly into the Town of Redkey's computer system and shall not otherwise be recorded .

(2) Each account shall be assigned an account number and personal identification number (PIN) which shall be unique to that account. The Town of Redkey may utilize computer software to randomly generate assigned PINs and to encrypt account numbers and PINs.

Section 6. 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 the Clerk Treasurer, 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 Clerk Treasurer and the password changed immediately.

(4) Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Clerk Treasurer.

Section 7. 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. Example 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 provided by a consumer reporting agency.*
- *d. Indications of a pattern of activity in a consumer report that is inconsistant with the history and usual pattern of activity of an applicant or customer, such as;*
  - *i. A recent and significant increase in the volume if inquires*
  - *ii. An unusual number of recently established credit relationships*
  - *iii. A material change in the use of credit, especially with respect to recently established credit relationships or*

iv. An account that was closed for cause or identified for abuse account privileges by a financial institution or creditor.

(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. Identificaion on which the information is inconsistent with information provided by the applicant or customer.

d. Identificaion on which the information in 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 institutions or creditor. For example:

i. The address does not match any address in the consumer report; 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 by the customer, such as a lack of correlation between the SSN range and date of birth.

c. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indcated by internal or third-party sources used by the financial institution or creditor.

d. Other information provided, such as fictitious mailing address, mail drop addresses , jail addresses, invalid phone numbers, pager numbers, pager numbers or answering services, is associated with fraudulent activity.

e. The SSN provided is the same as that submitted by other applicants or customers.

f. 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.

g. The applicant or customer fails to provide all required personal identifying information on an application or in response to notificaion that the application is incomplete.

h. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.

i. 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

ii. A material change in purchasing or spending patterns

d. An account that has been inactive for a long period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factore)

e. Mail sent to the customer in returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

f. Town of Redkey is notified that the customer is not receiving paper account statements.

g. Town of Redkey is notified of unauthorized charges or transactions in connection with a customer's account.

h. Town of Redkey is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identify theft.

(5) Notice from customers, law enforcement , victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts

Section 8. Prevention and Mitigation of Identity Theft.

(1) In the event that any employee resonsible for or involved in restoring an existing covered account or accepting payment for a covered account become aware of red flags indicating possible identity theft with respect to existing covered accounts, such employees shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identify theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediatey report such red flags to the Clerk-Treasurer. 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 President of the Town Council, who may in his or her discretion determinethat no further action is necessary. If the President of the Town Council 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 Clerk-Treasurer 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 a debt collector within 24 to 48 hours (not including weekends) of the discovery of likely or probable identity theft relating to a customer account that has beensold to such debt collector in the event that a customer's account has been sold to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;

e. 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

f. 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 identify 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 Clerk Treasurer. If, in his or her discretion , such employee deems that identity
theft is unlikely or that reliable informaton is available to reconcile red flags, the employee shall convey this information to the President of the Town Council, who may in his or her discretion determine that no further action is necessary. If the President of the Town Council in his or her discretion determines that further action is necessary, one or more of the following responses as determined to be appropriate shall be performed.

a. Request additional identifying informaton from the applicant;

b. Deny the application for new accounts;

c. Notify law enforcement of possible identity theft

d. Take other appropriate action to prevent or mitigate identify theft.

Section 9. Updating the Program.
The Town of Redkey shall annually review and, as deemed necessary, update the Identify 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 Town of Redkey and its covered accounts from identity theft. In so doing, the Town of Redkey shall consider the following factors and exercise its discretion in amending the program:

(1) The Town of Redkey's 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 entity) offers or maintains; and

(5) Updates in service provider arrangements.

Section 10. Program Administration.
The Clerk-Treasurer is responsible for oversight of the program and for program implementation. The Clerk Treasurer 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 Clerk-Treasurer 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 the Town Council.

The Clerk-Treasurer will report to the Town Council at least annually on compliance with red flag requirements. The report shall be due no later than May 1 of 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 Clerk-Treasurer 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 Clerk-Treasurer shall exercise his or her discretion in determining the amount and substance of training necessary.

Section 11. Outside Service Providers.
In the event that the Town of Redkey engages a service provider to perform an activity in connection with one or more covered accounts the Clerk Treasurer 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 12. Treatment of Address Discrepancies.
In the event that the Town of Redkey 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 Town of Redkey 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(1);
b. Information the Town of Redkey 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 Town of Redkey obtains from third party sources that are deemed reliable by the relevant employee; or

(2) Verify the information in the consumer report with the consumer.

Section 13. Furnishing Consumer's Address to Consumer Reporting Agency.
In the event that the Town of Redkey reasonably confirms that an address provided by a consumer is accurate, the Town of Redkey is required to provide such address to the consumer reporting agency from which it received a notice of address discrepancy with respect to such consumer. This information is required to be

provided to the consumer reporting agency when:

a. The Town of Redkey is able to form a reasonable belief that the consumer report relates to the consumer about whom it requested the report;

b. The Town of Redkey establishes a continuing relation with the consumer; and

c. The Town of Redkey regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.

Such information shall be provided to the consumer reporting agency as part of the information regularly provided by (the entity) to such agency for the reporting period in which the Town of Redkey establishes a relationship with the customer.

Section 14. 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 customer;

(2) Reviewing (the entity's) records to verify the consumer's address;

(3) Verifying the address through third party sources; or

(4) Using other reasonable processes

Section 15. Effective Date.
This ordinance shall become effective upon date of passage.

Dated this 23d day of April , 2009

Doug Stanley (signed)
Member

Dottie Quakenbush (signed)
Member

Phil Philebaum (signed)
Member

Terri Taylor (signed)
Member

Charlie Noble (Voted No)
Member

Attest;

Sandy Kirby (signed)
Clerk-Treasurer