CITY OF WHITING, INDIANA

IDENTITY THEFT PREVENTION PROGRAM

TABLE OF CONTENTS

Page

CITY OF WHITING, INDIANA

IDENTITY THEFT PREVENTION PROGRAM

Section 1 – Purpose.

The purpose of this document is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate Identity Theft in connection with the opening of a Covered Account or an existing Covered Account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (commonly known as "FACTA", Public Law 108-159).

Section 2 – Application.

This program shall apply to the Water Utility of the City for the protection of its customers against Identity Theft.

Section 3 – Definitions.

The following words and terms as used in this Program shall have the following meanings:

"Act" means the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159), as amended from time to time, including Part 681 of Title 16 of the Code of Federal Regulations implementing Section 114 and 315 thereof.

"Clerk-Treasurer" means the duly elected Clerk-Treasurer of the City of Whiting, Lake County, Indiana.

"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. Covered Accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and (ii) any other account that the financial institution or creditor offers or maintains for which there is an 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.

"Identify Theft" means a fraud committed or attempted using the identifying information of another person without authority.

"Program" means this Identity Theft Prevention Program, as amended from time to time.

"Red Flag" means a pattern, practice or specific activity that indicates the possible existence of Identity Theft. Red Flags include, but are not limited to, any of the following: (i) a fraud alert included with a consumer report; (ii) notice of a credit freeze in response to a request for a consumer report; (iii) consumer reporting agency providing a notice of address discrepancy; (iv) unusual credit activity, such as an increased number of accounts or

inquiries; (v) documents provided for identification appearing altered or forged; (vi) photograph on identification inconsistent with appearance of customer presenting the information; (vii) information on identification inconsistent with information provided by person opening account; (viii) (such as a signature card or recent check); (ix) application appearing forged or altered or destroyed and reassembled; (x) information on identification not matching any address in the consumer report; (xi) lack of correlation between social security number range and date of birth; (xii) personal identifying information associated with known fraud activity; (xiii) suspicious addresses supplied, such as a mail drop, or phone numbers associated with pages or answering service; (xiv) social security number provided matching that submitted by another person opening an account or other customers; (xv) an address or phone number matching that supplied by a large number of applicants; (xvi) the person opening the account unable to supply identifying information in response to notification that the application is incomplete; (xvii) personal information inconsistent with information already on file at Utility; (xviii) person opening account or customer unable to correctly answer challenge questions; (xix) shortly after change of address, Utility receiving request for additional users of account; (xx) customer fails to make first payment; (xxi) drastic change in payment patterns; (xxii) an account that has been inactive for a lengthy time suddenly exhibiting unusual activity; (xxiii) mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account; (xxiv) Utility notified that customer is not receiving paper account statements; (xxv) Utility notified of unauthorized charges or transactions on customer's account; (xxvi) Utility notified that they have opened a fraudulent account for a person engaged in identity theft.

"City" means the City of Whiting, Lake County, Indiana.

"City Administrator" means the responsible and identified head Administrative Employee for the City of Whiting, Lake County, Indiana.

"City Council" means the duly elected Legislative and Fiscal Body of the City of Whiting, Lake County, Indiana.

"Utility" means the water utility owner, operated and managed by the City pursuant to the provisions of Indiana Code 8-1.5-1-1 et seq., and all other applicable laws.

Unless defined above or otherwise indicated by the context in which they are used, the words and phrases in this Program shall have the meaning ascribed to them in the Act.

Section 4 – The Program

The City hereby establishes, solely in connection with the ownership, management and operation of its Utility, an Identity Theft Prevention Program to detect, prevent and mitigate Identity Theft. This Program hereby includes reasonable policies and procedures to:

1. Identify – Identify relevant Red Flags for Covered Accounts the City offers or maintains in connection with the ownership, management and operation of its Utility and incorporate those Red Flags into this Program;

2. Detect – Detect Red Flags that have been incorporated into this Program;

3. Respond – Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

4. Update – Ensure this Program is updated periodically to reflect changes in risks to Utility customers and to the safety and soundness of the Utility of the City, as the creditor, from Identity Theft.

This Program shall, as appropriate, incorporate existing policies and procedures of the City and the Utility that control reasonably foreseeable risks.

Section 5 – Administration of Program.

The Board of Public Works and Safety acting as the Whiting Municipal Waterworks Board shall be responsible for the overall development, implementation, oversight and continued administration of this Program. The City Administrator and Clerk-Treasurer shall be responsible for the day to day activities concerning said development, implementation, oversight and administration of this Program. The City Administrator and Clerk-Treasurer, with the oversight of the City Council, shall coordinate the training of Utility staff, as necessary, to effectively implement this Program. The City Council, in carrying out this Program, shall exercise appropriate and effective oversight of any service provider arrangements.

Section 6 – Identification of Relevant Red Flags.

This Program includes relevant Red Flags from the following categories as appropriate:

1. Alerts – Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services (see items (i) thru (iv) under the definition of Red Flag);

2. Suspicious Documents – The presentation of suspicious documents (see items (v) thru (ix) under the definition of Red Flag);

3. Suspicious Identification – The presentation of suspicious personal identifying information when compared against external information sources used by the Utility, such as suspicious address (see items (x) thru (xviii) under the definition of Red Flag);

4. Suspicious Activity – The unusual use of, or other suspicious activity related to, a Covered Account (see items (xix) thru (xxvi) under the definition of Red Flag); and

5. Notice – Notice from customers victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with Covered Accounts.

This Program shall consider the following risk factors in identifying relevant Red Flags for Covered Accounts as appropriate:

1. Types of Covered Accounts – The types of Covered Accounts offered or maintained in connection with the Utility.

2. Methods to Open – The methods provided by the Utility to open Covered Accounts;

3. Methods to Access – The methods provided by the Utility to access Covered Accounts; and

4. Previous History – The prior history and experience of the Utility and the City with identity theft.

This Program incorporates relevant Red Flags from sources such as:

1. Prior Incidents – Incidents of identity theft previously experienced by the Utility and the City;

2. Changes in Risk – Methods of identity theft that reflect changes in risk; and

3. Supervision – Applicable supervisory guidance.

Section 7 – Detection of Red Flags.

This Program addresses the detection of Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts, such as by:

1. Identifying Information – Obtaining identifying information about, and verifying the identity of, a person opening a Covered Account; and

2. Verification – Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing Covered Accounts.

Section 8 – Response.

This Program provides appropriate responses to detected Red Flags to prevent and mitigate Identity Theft. The response shall be commensurate with the degree of risk posed. Appropriate responses include:

1. Monitoring – Monitoring a covered Account for evidence of identity theft;

2. Customer Contact – Contacting the customer (contact may be made by e-mail, certified mail or telephone to the affected customer);

3. Change Passcodes – Changing any passwords, security codes or other security devices that permit access to a Covered Account;

4. New Account Number – Reopening a Covered Account with a new account number;

5. Not Open – Not opening a new Covered Account;

6. Close – Closing an existing Covered Account;

7. Notify Law Enforcement – Notifying the City's Police Department and any other necessary law enforcement personnel; or

8. Not Respond – Determining that no response is warranted under the particular circumstances.

Any Utility staff employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must first and immediately notify the City Administrator and Clerk-Treasurer. The City Administrator and Clerk-Treasurer will then determine the appropriate response in accordance with one (1) or more of the options above.

In the event notification to a customer is necessary, such notification shall include relevant information related to the incident including (i) the type of identifying information involved; (ii) the telephone number that the person can call for further information and assistance; (iii) local law enforcement contact information; and (iv) Federal Trade Commission contact information (877-438-4338 or www.consumer.gov/idtheft).

Section 9 – Updating the Program.

At the advisement of the City Administrator and/or the Clerk-Treasurer, the City Council shall update this Program periodically to reflect changes in risks to customers of the Utility or to the safety and soundness of the Utility and its customers from Identity Theft based on factors such as:

1. Experience – The experiences of the Utility and City with Identity Theft;

2. Changes in Methods – Changes in methods of Identity Theft and in methods to detect, prevent and mitigate Identity Theft;

3. Changes in Accounts – Changes in the types of accounts that the Utility offer or maintain;

4. Changes in Business – Changes in the business arrangements of the Utility, including acquisitions, alliances and service provider arrangements.

Section 10 – Oversight of the Program.

The oversight of this Program shall be undertaken by the City Administrator and Clerk-Treasurer. Such oversight shall include:

1. Staffing – Assignment of specific responsibility for implementation of the Program to appropriate Utility staff – the City Administrator and Clerk-Treasurer shall be responsible for the day to day administration of this Program and shall report directly to the City Council in connection with any matters relating to this Program;

2. Review of Reports – Review of reports prepared by staff regarding compliance – such reports to be presented by the City Administrator and Clerk-Treasurer to the City Council; and

3. Approval of Program Changes – Approval of material changes to this Program as necessary to address changing risks of Identity Theft.

Reports shall be prepared as follows:

1. Annual Report – the City Administrator and Clerk-Treasurer, responsible for the day to day development, implementation and administration of the Program, shall report to the City Council at least annually on compliance by the Utility with the Program.

2. Content of Report – The report shall address material matters related to this Program and evaluate issues such as:

   (a) Effectiveness of the 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;

   (b) Service Provider agreements;

   (c) Significant incidents involving Identity Theft and management's response;

   (d) Recommendations for material changes to this Program.

Section 11 – Oversight of Service Provider Arrangements.

The Utility shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft whenever the Utility or Utilities engage(s) a service provider to perform an activity in connection with one (1) or more Covered Accounts. For example, if the Utility determines to outsource business functions such as payroll, web hosting, customer call center operations, data process, or the like, the outsourcing company's data security practices will be compared with the Utility to assure adequate security measures are in place to detect, prevent and mitigate Identity Theft. Service providers shall be required to notify the Utility of any security incidents they experience which might result in or create a risk of Identity Theft of any of the Utilities' customers.

Section 12 – Duties Regarding Address Discrepancies.

The Utility shall develop policies and procedures designed to enable the Utility to form a reasonable belief that a credit report relates to the customer for whom it was requested if the Utility receive a notice of address discrepancy from a nationwide consumer reporting agency indication the address given by the customer differs from the address contained in the consumer report. The Utility may reasonable confirm that an address is accurate by any of the following means:

1. Verification with Customers – Verification of the address with the customer;

2. Record Review – Review of the Utilities' records;

3. Third-Party Verification – Verification of the address through third-party sources;

4. Other Means – Other reasonable means.

If an accurate address is confirmed, the Utility shall furnish the address of the customer to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. Customer Relationship – The Utility establishes a continuing relationship with the customer; and

2. Information – The Utility regularly and in the ordinary course of business furnishes information to the consumer reporting agency.

Section 13 – Security of Personal Identifying Information.

All paperwork documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable customers information (such as name, social security number, date of birth, driver's license number, alien registration number, passport number, employer tax identification number, and the like) will be stored in a locked file cabinet or cabinets. File cabinets containing personally identifiable customer information will be stored in a locked room. The City Administrator and Clerk-Treasurer will control keys to the file cabinet and room and will only distribute keys to those employees of the Utility with a legitimate need for such customer information.

Personal identifying customer information will be kept in locked file cabinets except when an employee is working on the file. Employees are not to leave such information on their desks in plain view when they are away from their workstations. At the end of the day, employees will put files containing personally identifiable customer information away in locked file cabinets. To the extent the Utility maintains personal identifying customer information in offsite storage facilities, access to such facilities will be limited to employees needing access to such information and visits to such facilities shall be documented.

Visitors who visit the Utilities' offices and who must enter areas where personally identifiable customer information or other sensitive information is kept shall be escorted by an employee of the Utility.

The Utility shall take appropriate measures to assure that personal identifying customer information contained on computers in the Utilities' offices or on laptops of the Utility will be reasonably protected (e.g., passwords, encryption, firewalls and the like).

Section 14 – Employee Training.

The City Administrator and Clerk-Treasurer shall periodically explain and train the staff of the Utility as to the contents of this Program and the need to spot security vulnerabilities.

New employees of the Utility shall be required to review this Program as part of their initial training. Access to a customer's personal identifying customer information will be limited to employees with a "need to know". Employees who leave employment of the Utility shall no longer have access to personal identifying customer information. The City Administrator and Clerk-Treasurer shall instruct employees to immediately notify him/her of any potential security breaches. Employees who violate the security policies of the Utility, including this Program, shall be subject to discipline up to and including dismissal.

Section 15 – Disposal of Sensitive Information.

Sensitive information such as personal identifying customer information that is no longer needed by the Utility shall be disposed of in a manner to assure the safeguarding of such information (e.g., shredding, incineration, permanent deletion).

ALL OF WHICH IS APPROVED AND ADOPTED THIS 20TH DAY OF APRIL, 2009.

CITY OF WHITING BOARD OF PUBLIC WORKS AND SAFETY ACTING AS THE WHITING MUNICIPAL WATERWORKS BOARD:

_____
Joseph M. Stahura, Mayor/President

_____
Marty Jakubowski, Member

_____
Mark Harbin, Member

ATTEST: _____
Mark S. Adam, Clerk-Treasurer