

**WEST CENTRAL CONSERVANCY DISTRICT
RESOLUTION NO. 09-02**

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST CENTRAL CONSERVANCY DISTRICT APPROVING AND IMPLEMENTING THE DISTRICT'S IDENTITY THEFT PREVENTION PROGRAM.

WHEREAS, the District is a utility operating a wastewater treatment collection and treatment system in Hendricks County, Indiana;

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003 require "Creditors" to adopt a written program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts;

WHEREAS, the Federal Trade Commission and other regulatory agencies of the federal government have adopted rules implementing the Act's mandates (the "Red Flag Rules");

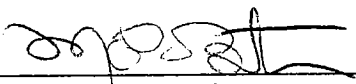
WHEREAS, the District is a Creditor, as that term is defined in the Federal Trade Commission's Red Flag Rules;

WHEREAS, the District's staff has consulted with the District's attorney and has developed a written program that satisfies the requirements of the Act and the Red Flag Rules (the "Program"); and

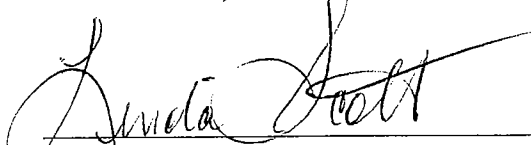
WHEREAS, the Board, having determined the Program to be appropriate to the size and complexity of the District and the nature and scope of its activities, finds it appropriate to approve the Program.

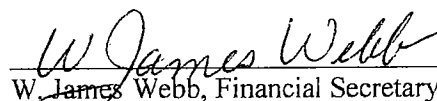
NOW, THEREFORE, BE IT RESOLVED, by the Board of Directors of the West Central Conservancy District that the Program is hereby approved, and that the District shall implement and administer the Program according to its terms.

Passed and adopted by the Board of Directors of the West Central Conservancy District on the 13th day of April, 2009.


Karl P. Buetow, Chairman


Paul E. Allen, Vice-Chairman


Linda L. Scott, Secretary


W. James Webb, Financial Secretary

William E. Holland, Member
1011583

**IDENTITY THEFT PROTECTION PROGRAM
OF
WEST CENTRAL CONSERVANCY DISTRICT**

MAY 1, 2009

I. PROGRAM ADOPTION

The West Central Conservancy District, a conservancy district duly authorized and formed under Indiana Code 14-33 ("***District***"), developed this Identity Theft Prevention Program ("***Program***") pursuant to the requirements of the U.S. Federal Trade Commission's Red Flags Rule¹ ("***Rule***"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.² This Program was developed with the oversight and approval of the District's Board of Directors. After consideration of the size and complexity of the District's operations and account systems, and the nature and scope of the District's activities, the District's Board of Directors determined that this Program was appropriate for the District, and therefore approved this Program as of May 1, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling Requirements Under the Rule

Under the Rule, a utility is subject to the Rule's requirements, including the establishment of an "***Identity Theft Prevention Program***" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing District covered accounts and incorporate those Red Flags into the Program.
2. Detect Red Flags that have been incorporated into the Program.
3. Respond appropriately to any detected Red Flags to prevent and mitigate Identity Theft.
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the District's safety and soundness from Identity Theft.

B. Red Flags Rule Definitions Used in This Program

The Rule defines "***Identity Theft***"³ as "fraud committed using the identifying information of another person," and a "***Red Flag***" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft." The District, as a utility, is a defined "***creditor***" under the Rule. As such, all of the District's accounts that are individual service accounts held by the District's customers, whether residential, commercial or industrial, are covered by the Rule if they qualify as covered accounts.

¹ 16 C.F.R. § 681.2 (2007).

² 15 U.S.C.A. § 1681m. (2003).

³ 16 C.F.R. § 603.2 (2004).

The Rule defines a “*covered account*” as (i) any District account offered or maintained primarily for personal, family or household purposes, that involves multiple payments or transactions, and (ii) any other District account offered or maintained for which there is a reasonably foreseeable risk to customers or the District’s safety and soundness from Identity Theft.

The Rule defines “*identifying information*”⁴ as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address, or routing code.

The rule defines “*service provider*” as a person that provides a service directly to a creditor.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the District has conducted an internal risk assessment considering the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. These included:

- Types of accounts offered and maintained by the District
- New accounts opened in person
- New accounts opened via telephone
- Account information accessed in person
- Account information accessed via telephone (person)
- Account information accessed via telephone (automated)
- Account information accessed via [District’s web site / worldwide web / Internet]

Based on such risk assessment, the District identified and adopts the following Red Flags, in each of the listed categories:

A. Suspicious Documents

Red Flags

- Identification document or card that appears to be forged, altered or inauthentic
- Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document
- Other document with information that is not consistent with existing customer information (such as if a person’s signature on a check appears forged)
- Application for service that appears to have been altered or forged

⁴ 16 C.F.R. § 603.2 (2004).

B. Suspicious Personal Identifying Information

Red Flags

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates)
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report)
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
- Social security number presented that is the same as one given by another customer
- An address or phone number presented that is the same as that of another person
- A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required)
- A person's identifying information is not consistent with information on file for customer
- The person attempting to open the covered account, or the customer inquiring about an existing account, cannot answer a challenging question asked by the District to authenticate the person or customer with information beyond that which generally would be available from a wallet or consumer report

C. Suspicious Account Activity or Unusual Use of Account

Red Flags

- Change of address for an account followed by a request to change the account holder's name
- Payments stop on an otherwise consistently up-to-date account
- Account used in a way that is not consistent with prior use (example: very high activity)
- Mail sent to the account holder is repeatedly returned as undeliverable
- Notice to the District that a customer is not receiving mail sent by the District
- Notice to the District that an account has unauthorized activity
- Breach in the District's computer system security
- Unauthorized access to or use of customer account information

D. Alerts from Others

Red Flag

- Notice to District from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, District personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

- Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification
- Verify customer's identity (for instance, review a driver's license or other identification card)
- Review documentation showing the existence of a business entity
- Independently contact the customer

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, District personnel will take the following steps to monitor transactions with an account:

Detect

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email)
- Verify the validity of requests to change billing addresses
- Verify changes in banking information given for billing and payment purposes

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event District personnel detect any identified Red Flags, such personnel shall coordinate with the Program Administrator (See Section VII(A)) to take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

- Notify the Program Administrator for determination of the appropriate step(s) to take
- Appropriate steps may include:
 - Continue to monitor an account for evidence of Identity Theft
 - Contact the customer
 - Change any passwords or other security devices that permit access to accounts
 - Not open a new account
 - Close an existing account
 - Reopen an account with a new number

- Not attempt to collect on a covered account or not sell a covered account to a service provider until reasonable steps have been taken to authenticate the account (See Section IV)
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances

Protect Customer Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to District accounts, the District will take the following steps with respect to its internal operating procedures to protect customer identifying information:

- Ensure that District website is secure or provide clear notice that website is not secure
- Ensure complete and secure destruction of paper documents and computer files containing customer information
- Ensure that District office computers are password protected and that computer screens lock after a set period of time
- Keep any District offices accessible to the public or employees who have not completed training under this program clear of papers containing customer information
- Ensure District computer virus protection is up to date
- Require and keep only kinds of customer information that are necessary for District purposes
- Dispose of any other customer information in a manner that complies with the District's record retention obligations and prevents access to the customer information by any third person

VI. PROGRAM UPDATES

The Program Administrator will review and update this Program on an annual basis to reflect changes in risks to customers and the soundness of the District from Identity Theft. In doing so, the Program Administrator will consider the District's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the District's business arrangements with other entities. In conjunction with such review, the Program Administrator will prepare and submit to the Board of Directors a report summarizing matters 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 responses to them, and recommendations for substantial changes to the Program, if any. The report shall include the Program Administrators recommended changes, if any. Upon review and consideration of such report, the Board of Directors will determine whether changes to the Program, including the listing of Red Flags, are warranted.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with a Program Administrator, who shall be the Assistant District Manager. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of District staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

District staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements

In the event the District engages a service provider to perform an activity in connection with one or more District accounts, the District will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

- Require, by contract, that service providers have such policies and procedures in place
- Require, by contract, that service providers review the District's Program and report any detected Red Flags to the Program Administrator.

D. Non-disclosure of Specific Practices

For the effectiveness of this Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to the Identity Theft Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered public records excepted from public access under Indiana Code 5-14-3-4.