



Policy 24 – Identity Theft Prevention Program

IDENTITY THEFT PREVENTION PROGRAM

OF WEBB CREEK UTILITY DISTRICT

The Utility maintains accounts for its customers to pay for utility service where bills are sent and payments are due monthly. These accounts are covered accounts under the Red Flag Rules adopted by the Federal Trade Commission (FTC) in 16 C.F.R. § 681.2. The Utility adopts this identity theft Prevention Program (the Program) to comply with 16 C.F.R. § 681.2 which is designed to detect, prevent and mitigate identity theft in connection with these customer accounts. The accounts covered by this Program shall be referred to as customer accounts.

SECTION I. IDENTIFICATION OF RELEVANT RED FLAGS

A. Risk Factors. In identifying relevant Red Flags associated with customer accounts, the Utility's Board of Commissioners and management have considered the following identity theft risk factors:

1. Types of Covered Accounts – The Utility opens and maintains customer accounts for persons to pay for utility service rendered where bills are sent and payments are due monthly which are covered accounts.
2. Methods for Opening Accounts. The Utility requires that persons or businesses which wish to receive utility service submit an application for utility service with the following information:
 - (1) full legal name;
 - (2) address location where service shall be provided;
 - (3) mailing address if different than service address;
 - (4) contact and billing information;

The applicant for service may be required to present to the customer service employee a valid government-issued photo identification as proof of identity.

3. **Methods for Accessing Accounts.** The Utility allows customers to access information related to their accounts using the following methods:

- (a) in person at the Utility office with a proper identification;
- (b) over the telephone after providing the customer service employee with certain identifying information such as any of the following: the address and telephone number of the service location,

4. **Previous Experience with Identity Theft.** The Utility is not aware of any security breach of or unauthorized access to its system used to store customers' identifying information. The historical absence of identity theft of its customers' information is due to (1) the limited services and credit provided to its customers, both of which are tied to an immovable physical location; (2) the minimal size of the population it serves; (3) the relatively low rate of change in customer base; and (4) the Utility's procedures for securing customers' personal information.

B. **Sources of Red Flags.** In identifying relevant Red Flags associated with customer accounts, the Utility's Board of Commissioners and management have considered the following sources of Red Flags for identity theft:

1. **Past Incidents of Identity Theft.** As described in Section I.A.4 above, the Utility is not aware of any security breach of or unauthorized access to its system used to store customers' personal identifying information collected by the Utility. In the event of incidents of identity theft in the future, such incidents shall be used to identify additional Red Flags, and this Program will be amended accordingly.

2. **Identified Changes in Methods of Identity Theft.** The Utility will review methods of identity theft it has identified to assess changes in identity theft risks.

3. **Applicable Supervisory Guidance.** As a part of its annual review, the Utility will review additional regulatory guidance from the FTC and other consumer protection authorities on new identity theft risks and recommended practices for identifying, detecting, and preventing identity theft

C. **Categories of Red Flags.** In identifying relevant Red Flags associated with customer accounts, the Utility's Board of Commissioners and management have considered the following categories of Red Flags for identity theft.

1. **Suspicious Documents.** The presentation of suspicious documents can be a Red Flag for identity theft. Presentation of suspicious documents includes:

- (a) Documents provided for identification that appear to have been altered or forged;
- (b) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
- (c) Other information on the identification is not consistent with information provided by the person opening a new account or the customer presenting the identification;
- (d) Other information on the identification is not consistent with readily accessible information that is on file with the Utility such as the customer's application for service; and
- (e) An application for service appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

2. Suspicious Personal Identifying Information. The presentation of suspicious personal identifying information can be a Red Flag for identity theft. Presentation of suspicious personal identifying information occurs when:

- (a) Personal identifying information provided is inconsistent when compared against external information sources used by the Utility;
- (b) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer;
- (c) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Utility, for example:
 - (1) The address on an application for service is the same as the address provided on a fraudulent application; or
 - (2) The phone number on an application is the same as the number provided on a fraudulent application.
- (d) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Utility. For example:

(1) The address on an application is fictitious or a mail drop;
or

(2) The phone number is invalid or is associated with a pager
or answering service.

(e) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

(f) The person opening the covered account or the customer fails to provide all required personal identifying information on an application for service or in response to notification that the application is incomplete.

(g) Personal identifying information provided is not consistent with personal identifying information that is on file with the Utility.

(h) The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. **Suspicious Activity.** The unusual use of or other suspicious activity related to a customer account can be a Red Flag for identity theft. Suspicious activities include:

(a) Shortly following the notice of a change of address for a customer account, the Utility receives a request for the addition of other persons to be served at the address on the account.

(b) A customer fails to make the first payment or makes an initial payment but no subsequent payments on the account.

(c) A customer account is used in a manner which is not consistent with established patterns of use on the account such as:

(1) Nonpayment when there is no history of late or missed payments; or

(2) A material change in the amount of utility service purchased;

(d) Mail sent to the customer is returned repeatedly as undeliverable although utility purchases continue to be made on the customer account.

(e) The Utility is notified that the customer is not receiving paper account statements.

5. Notices. Notices of potential identity theft are serious Red Flags which notices shall include:

(a) Notice from customers, law enforcement authorities or other persons indicating that a customer may have been a victim of identity theft;

(b) Notice to the Utility that a customer has provided information to someone fraudulently claiming to represent the Utility;

(c) Notice to the Utility that a fraudulent website which appears similar to the Utility's website is being used to solicit customer personal identifying information;

(d) The Utility's mail servers are receiving returned e-mails that the Utility did not send indicating that a customer may have received fraudulent e-mail soliciting customer personal identifying information.

SECTION II. DETECTING RED FLAGS

A. The Utility shall obtain identifying information about a person opening a customer account and shall verify the identity of the person opening a customer account. The Utility will obtain the following information to open a customer account:

- (1) name full legal name;
- (2) address location where service shall be provided;
- (3) mailing address if different than service address;
- (4) contact and billing information.

The applicant for service may be required to present to the Utility customer service employee a valid government-issued photo identification as proof of identity.

B. The Utility shall not provide identifying information to its customers, either verbally or in writing, even when a customer is asking for the customer's own information.

C. For existing customer accounts the Utility shall authenticate customers, monitor transactions and verify the validity of change of address requests.

SECTION III. PREVENTING AND MITIGATING IDENTIFY THEFT

A. If a Utility employee detects a Red Flag on a customer account, the Utility employee shall notify the employee's supervisor or the General Manager that the employee has detected a Red Flag. The General Manager may take the following steps to prevent identity theft:

- (1) Monitoring a customer account for evidence of identity theft;
- (2) Changing any passwords, security codes, or other security devices that permit access to a customer account;
- (3) Reopening a customer account with a new account number;
- (4) Closing an existing customer account;
- (5) Not attempting to collect on a customer account;
- (6) Notifying the customer;
- (7) Notifying law enforcement; or
- (8) Determining that no response is warranted under the particular circumstances.

B. If the Utility discovers that any of its customers have become victims of identity theft, the Utility shall notify the customer and local law enforcement.

SECTION IV. PROGRAM UPDATES AND ADMINISTRATION

The Utility shall update the Program at least annually to reflect changes in risks to customers of identity theft. In updating the Program, the Utility shall consider the following:

- A. the Utility's experiences with identity theft;
- B. changes in methods of identity theft;
- C. changes in methods to detect, prevent, and mitigate identity theft;
- D. changes in the Utility's types of customer accounts.

SECTION V. PROGRAM ADMINISTRATION

A. The Program shall be approved by the Board of Commissioners. The General Manager shall oversee the administration of the Program. The General

Manager may assign specific responsibility for the implementation of the Program to Utility employees. The General Manager shall review reports prepared by Utility employees under subsection V.B.

B. The General Manager shall prepare and present a written report to the Board of Commissioners at least annually on the Utility's compliance with 16 C.F.R. § 681.2. The report to the Board of Commissioners shall include a discussion of the following:

1. the effectiveness of the Program in addressing the risk of identity theft;
2. third party service provider arrangements;
3. significant incidents of identity theft and management's response; and
4. recommendations for changes to the Program.

The General Manager's annual report shall be incorporated into the minutes of the Board of Commissioners meeting at which the report is given.

C. The Utility has business relationships with third party service providers for billing services, meter reading, backflow prevention, maintaining a secure website, collection of delinquent accounts and other services. Under these business relationships, the third party service providers have access to customer identifying information covered under this Program. The General Manager shall ensure that a third party service providers' work for the Utility is consistent with this Program by:

- (1) Amending contracts with the third party service providers to incorporate these requirements; or
- (2) Determining that the third party service providers have reasonable alternative safeguards that provide the same or a greater level of protection for customer information as provided by the Utility.

IV. EFFECTIVE DATE

October 3, 2008