



KOOTENAI-PONDERAY SEWER DISTRICT

IDENTITY THEFT PREVENTION PROGRAM

KOOTENAI-PONDERAY SEWER DISTRICT

IDENTITY THEFT PREVENTION PROGRAM

In order to help combat identity theft, Congress enacted section 114 of the Fair and Accurate Transaction Act of 2003 (FACTA). In accordance with the Rules adopted by the Federal Trade Commission to implement FACTA, the District, as a utility provider that allows its customers to pay for utility services after the services have been received, is required to adopt an Identity Theft Prevention Program to protect its utility customers.

The following policies and procedures are for the purpose of detecting, preventing and mitigating identity theft. The policies and procedures take into account the size and complexity of the District's utility operations and account systems, and the nature and scope of the District's utility activities.

For the purpose of this Program, the following definitions will apply:

"Covered Account" -

1. Any account the District offers or maintains primarily for personal, family, or household purposes, that involves multiple payments or transactions; and
2. Any other account the District offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the District from identity theft.

"Identifying Information" -

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 Internet Protocol address, or routing number.

I. IDENTIFYING RED FLAGS:

The following are identified as *Red Flags*, which are potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification.

Alerts, Notifications, or Warnings from a Consumer Reporting Agency, including but not limited to the following examples:

1. A fraud or active duty alert included with a consumer report.
2. A notice of credit freeze from a consumer reporting agency in response to a request by the District for consumer report.
3. A notice of address discrepancy from a consumer reporting agency as defined in §334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

4. A consumer report that indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a creditor.

Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the District, such as a signature card or recent check.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the District. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or the number is listed on the Social Security Administration's Death Master File.
2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the District. For example:
 - a. The address on an application is fictitious, a mail drop, or a prison; or

- b. The phone number is invalid, or is associated with a pager or answering service.
4. The SSN provided is the same as that submitted by other persons opening an account or other customers.
5. 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.
6. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
7. Personal identifying information provided is not consistent with personal identifying information that is on file with the District.
8. The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report in the event that the District elects to include as part of the account application the requirement for the applicant to provide the answer to a challenge question to be used to verify the identity of the customer when asking for information.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

1. A new account is used in a manner commonly associated with known fraud patterns. For example:
 - a. The customer fails to make the first payment or makes an initial payment but no subsequent payments
2. The District is notified that the customer is not receiving paper account statements.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Creditor.

1. The District is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the District has opened a fraudulent account for a person engaged in identity theft.

Incidents of identity theft that the District has experienced

1. The customer's behavior, or the information provided by the customer, is consistent or similar to that of other customers that the District has experienced as having been relating to incidents of identity theft.

2. Other patterns of behavior that the District experiences from time-to-time that have been used in identity theft.

II. PROCEDURES TO DETECT RED FLAGS

Verify Identity

1. Utility customers will be required to provide sufficient information to identify them as the owner of the property for which the utility services are to be provided.
2. Utility accounts will not be transferred into the name of a new customer without obtaining the same verification as required for the initial service request.
3. Utility accounts must be in the name of the property owner and not in the name of the tenant, unless allowed by District ordinance and there is a written agreement signed by both the tenant and the property owner that the property owner will be jointly responsible for payment of the account.
4. If the mailing address for the account is not the same address as the property receiving the services, the customer must provide verification that the mailing address is valid.

III. PROCEDURES TO PREVENT AND MITIGATE IDENTITY THEFT

1. Any time a Red Flag is identified relating to a covered account, the information will be provided to the persons assigned to administer this Program (Program Administrator). The Program Administrator will review the information and determine, in consultation with the Board and the District's Attorney when appropriate, which of the following steps shall be followed:
 - a. Continued monitoring of the account for evidence of identity theft;
 - b. Contact the customer at the address where the services are being received to verify the information and/or identity of the customer;
 - c. Change any passwords or other security devices, if any are used by the District, which would permit access to accounts.
 - d. Refuse to establish the account in the name of the person requesting the account be opened or the name on the account be changed;
 - e. Close an existing account;
 - f. Reopen an account with a new number;
 - g. Notify law enforcement; or
 - h. Determine that no response is warranted under the particular circumstances.

IV. PROGRAM ADMINISTRATION

Program Administrator

The District's Treasurer-Business Office Manager, or the Treasurer-Business Office Manager's designee, shall serve as the Program Administrator under the direction of the Board of Directors of the Kootenai-Ponderay Sewer District.

Duties of the Program Administrator

The Program Administrator shall have the following duties:

1. Developing, implementing and updating this Program;
2. Administration of this Program;
3. Ensuring that the District's staff is appropriately trained;
4. Reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft;
5. Determining which steps for prevention and mitigation should be taken in particular circumstances; and
6. Considering periodic changes to the Program.

Staff Training and Reports

1. District staff responsible for implementing this 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.
2. Staff should prepare a report at least annually for the Program Administrator, including but not limited to the following:
 - a. An evaluation of the effectiveness of the Program with respect to opening accounts;
 - b. An evaluation of existing covered accounts;
 - c. An evaluation of service provider arrangements;
 - d. Significant incidents involving identity theft and response; and
 - e. Recommendations for changes to the Program.

Service Provider Arrangements

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

1. Require, by contract, the service provider to have such policies and procedures in place; and
2. Require, by contract, the service provider review this Program and report any Red Flags to the Program Administrator.

V. PERIODIC UPDATING OF THE PROGRAM

This Program will be reviewed by the Program Administrator at least annually to determine if the Program needs to be amended to reflect changes in risks to customers and to determine the soundness of the Program to protect District covered accounts from identity theft. The review shall include at least the following:

1. Additions or modifications to the Red Flags, based on the following:
 - a. The District's experience with identity theft;
 - b. New information regarding Red Flags from other sources, including but not limited to, credit reporting agencies and law enforcement.
2. Changes in methods of identity theft.
3. Changes in methods to detect, prevent and mitigate identity theft.
4. Changes in business arrangements.
5. Changes in types of accounts offered.
6. Changes in the District's utility business arrangements with other entities.

If the Program Administrator determines that updates to this Program are warranted, the Program Administrator will make recommendations for changes to the District's Board of Directors. The Board of Directors may accept, modify, or reject those recommended changes to this Program.