


CERTIFICATE AS TO RESOLUTION AND ADOPTING VOTE

I, the undersigned, being the duly qualified and acting recording officer of Big Sky County Water & Sewer District No. 363, Montana (the "District"), hereby certify that the attached resolution is a true copy of a Resolution entitled: "A RESOLUTION OF BIG SKY COUNTY WATER & SEWER DISTRICT NO. 363, MONTANA, APPROVING AND ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM" (the "Resolution"), on file in the original records of the District in my legal custody; that the Resolution was duly adopted by the Board of Directors of the District at a regular meeting on August 16th, 2011 and that the meeting was duly held by the Board of Directors and was attended throughout by a quorum, pursuant to call and notice of such meeting given as required by law; and that the Resolution has not as of the date hereof been amended or repealed.

I further certify that, upon vote being taken on the Resolution at said meeting, the following Directors voted in favor thereof: Packy Cronin, Gary McRae, Dick Fast, Jeff Daniels, Bill Olson and Bill Shropshire; voted against the same: _____; abstained from voting thereon: _____; or were absent: Dick Allgood.

WITNESS my hand and seal officially this 16th day of August, 2011.





Dick Fast, Secretary

RESOLUTION NO. 11-01

A RESOLUTION OF BIG SKY COUNTY WATER & SEWER
DISTRICT NO. 363, MONTANA, APPROVING AND
ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Big Sky County Water & Sewer District No. 363, Montana (the "District") is a county water or sewer district, validly organized pursuant to Title 7, Chapter 13, Parts 21 and 22, M.C.A.; and

WHEREAS, the District was incorporated on August 5, 1993 and is located within the boundaries of Gallatin County and Madison County, political subdivisions of the State of Montana; and

WHEREAS, The Fair and Accurate Credit Transaction Act of 2003, Pub. L. 108-159, ("Red Flag Rule") requires certain financial institutions and creditors with "covered accounts" to prepare, adopt, and implement an identity theft prevention program to identify, detect, respond to and mitigate patterns, practices or specific activities which could indicate identity theft; and

WHEREAS, the District maintains certain continuing accounts with utility service customers and for other purposes which involve multiple payments or transactions, and such accounts are "covered accounts" within the meaning of Red Flags Rule; and

WHEREAS, to comply with the Red Flags Rule, District Staff have prepared an identity theft prevention program in the form attached hereto as Exhibit "A" and incorporated herein by this reference (the "ITPP" or the "Program") and have recommended that the Program now be approved and adopted by the District Board of Directors for implementation; now, therefore

BE IT RESOLVED by the Board of Directors (the "Board") of the District as follows:

1. The Program is hereby approved and adopted effective the date set forth below.
2. District Staff are hereby authorized and directed to implement the Program in accordance with its terms.

Passed and approved this 16th day of August, 2011.



Packer Cronin, President, Board of Directors

Attest:



(SEAL)

Dick Fast, Secretary

EXHIBIT A

Big Sky County Water & Sewer District 363 Identity Theft Prevention Program

I. Program Adoption

The Big Sky County Water & Sewer District 363 developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s Red Flag Rule (“Rule”), which implements Sections 114 and 315 of the Fair and Accurate Credit Transaction Act of 2003. This Program was developed with the oversight and approval of the District Board of Directors and the District’s Finance Officer. After consideration of the size and complexity of the District’s activities. The District Board of Directors determined that this Program was appropriate for the District, and therefore approved this Program by the adoption of Resolution No.11-01 on the 16th day of August, 2011.

II. Program Purpose and Definitions

A. Fulfilling requirements of the Red Flag Rule

Under the Red Flags Rule, every financial institution and creditor is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags as defined in the Rule and this Program for new and existing 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 Red Flags that are detected to prevent and mitigate identity theft; and
4. Update the Program periodically to reflect changes in risks to customers or to the safety and soundness of the District from identity theft.

B. Red Flags Rule definitions used in the Program

For the purposes of this Program, the following definitions apply:

1. Account. “Account” means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.
2. Covered Account. A “covered account” means;
 - a. Any account the District offers or maintains primarily for business, personal, family or household purposes, that involves multiple payments or transactions; and

- b. Any other account the District offers or maintains for which there is a reasonably foreseeable risk to customer or to the safety and soundness of the District from Identity Theft.
3. Creditor. “Creditor” has the same meaning as defined in Section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a, and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the District.
4. Customer. A “customer” means a person or business entity that has a covered account with the District.
5. Financial Institution. “Financial institution” means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to a customer.
6. Identifying Information. “Identifying information” means 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 or unique electronic identification number.
7. Identity Theft. “Identity Theft” means fraud committed using the identifying information of another person.
8. Red Flag. A “Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
9. Service Provider. “Service provider” means a person or business entity that provides a service directly to the District relating to or connection with a covered account.

III. Identification of Red Flags.

In order to identify relevant Red Flags, the District shall review and consider the types of covered accounts that is offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft. The District identifies the following Red Flags, in each of the listed categories:

A. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Other document with information that is not consistent with existing customer information (such as a person’s signature on a check appears forged); and
3. Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides;
2. Identifying information presented that is the same as information shown on applications that were found to be fraudulent;
3. Identifying information presented that is consistent with fraudulent activity.
4. An address or phone number presented that is the same as that of another person;
5. Identifying information which is not consistent with the information that is on file for the customer.

C. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the District that an account has unauthorized activity;
6. Breach in the District's computer system security; and
7. Unauthorized access to or use of customer account information.

D. Alerts from Others

Red Flags

1. Notice to the District from a customer, a victim of identity theft, a law enforcement authority 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 Red Flags

1. Verify that the documentation from Title companies is valid. New accounts are only opened after property transfer through the sale or transfer of property. Title companies

send the warranty deed with the new owner information. The District relies on the accuracy for new account ownership on recorded documents.

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:

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

V. Preventing and Mitigating Identity Theft

In the event District personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of the risk posed by the Red Flag:

Prevent and Mitigate Identity Theft

1. Monitor a covered account for evidence of Identity Theft;
2. Contact the customer with the covered account;
3. Change any passwords or other security codes and devices that permit access to a covered account;
4. Not open a new covered account;
5. Close an existing covered account with a new number;
6. Reopen a covered account with a new number;
7. Not attempt to collect payment on a covered account;
8. Notify the Program Administrator for determination of the appropriate step(s) to take;
9. Notify law enforcement; or
10. 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 shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Secure the District website but provide clear notice that the website is not secure;
2. Undertake complete and secure destruction of paper documents and computer files containing customer information;

3. Make office computers password protected and provide that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer identifying information;
5. Maintain computer virus protection up to date; and
6. Require and keep only the kinds of customer information that are necessary for District purposes.

VI. Program Updates

The Program will be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the District from Identity Theft. The Program Administrator shall at least annually consider the District's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the District maintains and changes in the District's business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall update and implement the revised Program, present the Program Administrator's recommended changes to the District Board of Directors for review and approval.

VII. Program Administration

A. Oversight

The Program Administrator shall be responsible for developing, implementing and updating the Program.

A District Identity Theft Committee shall be responsible for developing, implementing and updating the Program. The Committee shall be comprised of the Program Administrator and Finance Officer appointed by the Program Administrator and Board of Directors.

The Program Administrator shall be responsible for the Program administration, for appropriate staff 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. District staff

will provide reports to the Program Administrator on any incidents of Identity Theft.

C. Service Provider Arrangements

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

1. Require, by contract, that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to District covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program; or
2. Require, by contract, that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to District covered accounts in compliance with the terms and conditions of the service provider's identity theft prevention program and will take appropriate action to prevent and mitigate identity theft; and that the service providers agree to report promptly to the District in writing if the service provider in connection with a District covered account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.

D. Customer Identifying Information and Public Disclosure

The identifying information of District customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law. The District Board of Directors also finds and determines that public disclosure of the District's specific practices to identify, detect, prevent and mitigate identify theft may compromise the effectiveness of such practices and hereby directs that, under the Program, knowledge of such specific practices shall be limited to the Program Administrator and the Identity Theft Committee and those District employees and service providers who need to be aware of such practices for the purpose of preventing Identity Theft.