RESOLUTION NO. 10
SERIES 2008

A RESOLUTION ADOPTING A RED FLAG POLICY AND ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM FOR THE TOWN OF CRESTED BUTTE

WHEREAS, pursuant to federal law the Federal Trade Commission ("FTC") has issued regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs (the "Red Flag Rules"); and

WHEREAS, the Town of Crested Butte is a municipal utility provider, and, as such, is a "creditor" as defined in the Red Flag Rules; and

WHEREAS, pursuant to the Red Flag Rules, the Town must identify and detect relevant warning signs, describe responses to prevent and mitigate identity theft, detail a plan to update the program, and include appropriate training and oversight; and

WHEREAS, in compliance with the Red Flag Rules, the Town of Crested Butte desires to create and adopt an appropriate identity theft prevention program.

NOW, THEREFORE, BE IT RESOLVED BY THE TOWN COUNCIL OF THE TOWN OF CRESTED BUTTE, COLORADO, THAT:

The Red Flag Policy attached as Exhibit A is hereby adopted and approved and shall be in full force and effect upon its passage and adoption.

INTRODUCED, READ AND ADOPTED THIS THIRD DAY OF NOVEMBER, 2008.

Alan Bernholtz, Mayor

ATTEST:

Eileen Hughes, Town Clerk

TOWN OF CRESTED BUTTE CORPORATE SEAL JULY 2, 1880 GUNNISON COUNTY, CO

EXHIBIT A
Red Flag Policy and Identity Theft Prevention Program

Purpose

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 (FACTA) of 2003.

Definitions

1. *Covered Account* means 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; or any other account that the financial institution or creditor offers or maintains for which there is a 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.

2. *Identity Theft* means fraud committed or attempted using the identifying information of another person without authority.

3. *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Findings

1. The Town is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.

2. Covered accounts offered to customers for the provision of Town services include utility accounts.

3. The process of opening a new covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur.

4. The Town limits access to personal identifying information to those employees responsible for or otherwise involved in opening covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered directly into the Town's computer system and is not otherwise recorded.

5. The Town determines that there is a low risk of identity theft occurring in the following ways:

    a. Use by an applicant of another person's personal identifying information to establish a new covered account; and
    b. Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts.

Access to Covered Account Information

1. Access to customer accounts shall be password protected and shall be limited to authorized Town personnel.

2. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Finance Officer and the password changed immediately.

3. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Town Clerk under open records law.

Credit Card Payments

1. In the event that credit card payments that are made over the Internet are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.

2. All credit card payments made over the telephone or the Town's web site shall be entered directly into the customer's account information in the computer database.

3. Account statements and receipts for covered accounts shall not include the credit or debit card or the bank account used for payment of the covered account.

Identification of Red Flags

All employees responsible for or involved in the process of opening a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft. The following shall be considered Red Flags for the purpose of this policy:

a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
b. The presentation of suspicious documents;
c. The presentation of suspicious personal identifying information;
d. The unusual use of, or other suspicious activity related to, a covered account; and

e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Prevention and Mitigation of Identity Theft

Town employees responsible for opening covered accounts, accepting payments on a covered account or making changes to a covered account shall be responsible for the following actions:

a. Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
b. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

In the event a Town employee handling a covered account becomes aware of red flags indicating possible identity theft, they shall provide appropriate responses, commensurate with the degree of risk posed, to red flags that have been detected in order to prevent and mitigate identity theft. The appropriate responses may include any of the following:

a. Monitor a covered account for evidence of identity theft;
b. Contact the customer;
c. Change any passwords, security codes, or other security devices that permit access to a covered account;
d. Reopen a covered account with a new account number;
e. Not open a new covered account;
f. Close an existing covered account;
g. Notify law enforcement; or
h. Determine no response is warranted under the particular circumstances.

Program Updates

The Red Flag Policy and Identity Theft Prevention Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft. Factors upon which the updates will be based include the following:

a. The experiences of the Town 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 types of accounts that the Town offers or maintains;
e. Changes in the service provider arrangements of the Town.

Program Oversight

1. The Finance Director for the Town of Crested Butte shall be responsible for the development, implementation, oversight, and continued administration of this policy and program.

2. The Finance Director is responsible for providing training to staff, as necessary, to effectively implement the policy and program.

3. In the event the Town engages a service provider to perform an activity in connection with one or more covered accounts, the Finance Director shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.