CASTLE PINES
NORTH
METROPOLITAN DISTRICT

IDENTITY THEFT PREVENTION PROGRAM

Compliance with 16 C.F.R. Part 681
Fair and Accurate Credit Transactions Act
(FACT Act)

Approved by:
Castle Pines North Metro District
Board of Directors
On
April 20, 2009

CASTLE PINES NORTH METROPOLITAN DISTRICT
DOUGLAS COUNTY, COLORADO
RESOLUTION NO. 2009-004

Be it resolved that this is the policy of the Castle Pines North Metro District to maintain maximum compliance with the Fair and Accurate Credit Transaction (FACT) Act, its amendments, laws and regulations.

The Board of Directors designates Dan Schmick, Assistant District Manager, as the FACT Act Officer. The FACT Act officer is responsible for coordinating and monitoring day-to-day FACT Act compliance and managing all aspects of the FACT Act Identity Theft Prevention compliance program, including but not limited to adherence of FACT Act and its implementing regulations.

The Board of Directors will be ultimately responsible for the District's FACT Act compliance and will ensure that the FACT Act officer has sufficient authority and resources (monetary, physical and personnel) to administer an effective risk based FACT Act Identity Theft Prevention compliance program.

The FACT Act Identity Theft Prevention compliance program will include:

1. Approval of the written Program from the Board of Directors that directs management to create and implement a system of internal controls designed to:
    a. Identify Red Flags the District is likely to encounter;
    b. Document how the District's financial employees are to detect these Red Flags;
    c. Respond appropriately (risk based) to these Red Flags; and
    d. Ensure the Program is updated periodically.
2. Involvement of the Board of Directors or an appropriate committee or a designated senior level employee (a "FACT Act Officer") in the oversight, development, implementation and administration (to include annual report to the Board of Directors) of the Program;
3. Staff training and
4. Due diligence of service provider arrangements.

This policy was approved by the Board of Directors of the Castle Pines North Metro District on April 20, 2009.

President, William Santos

Janet C. Burnham
Secretary

I. Purpose

The policy is established to assist the Castle Pines North Metropolitan District and its employees to comply with the Fair and Accurate Credit Transactions Act, herein referred to as the FACT Act, by adhering to 16 C.F.R. Part 681 which prescribes duties for certain entities in preventing and mitigating identity theft in the conduct of their operations. The policy allows for the protection of sensitive customer information held within the District's account records and billing system. Primary focus is directed toward identifying Red Flags or account initiations, routine maintenance of existing accounts, and new activity on inactive or dormant accounts.

II. Definitions

1. **Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
2. **Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.
3. **Customer** means a person that has a covered account with a creditor.
4. **District or CPNMD** means the Castle Pines Metropolitan District.
5. **Identity theft** means a fraud committed or attempted using identifying information of another person without authority.
6. **Person** means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
7. **Personal identifying information** means a person's credit card account information, debit card information, bank account information and driver's license information and for a natural person includes their social security number, mother's birth name, and date of birth.
8. **Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
9. **Service provider** means a person that provides a service directly to the District.

III. Identifying Relevant Red Flags

The District will consider the following risk factors in identifying relevant Red Flags for covered accounts, as appropriate:

1. The types of covered account it offers or maintains;
2. The methods it provides to open its covered accounts;
3. The methods it provides to access its covered accounts; and
4. Its previous experiences, if any, with identity theft.

The District will incorporate Red Flags from sources such as:

1. Incidents of identity theft that the District has experienced;
2. Methods of identity theft that the District has identified that reflect changes in identity theft risks and
3. Applicable supervisory guidance, i.e., state accounting and auditing rules.

The categories of Red Flags will include but are not limited to:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services:
2. The presentation of suspicious documents;
3. The unusual use of, or other suspicious activity related to, a covered account; and
4. 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 District.

IV. Detecting Red Flags

In the course of the District's routine handling of new or existing accounts, the District shall:

1. Obtain customer identifying information from the customer, title company, builder, landlord, or management company prior to opening a customer account;
2. Require a completed application and copy of a voided check to enroll a customer into the automatic bill payment (ACH)

V. Responding to Red Flags

The District will document an appropriate response to each Red Flag the District or a customer has detected, commensurate with the degree of risk perceived. In determining an appropriate response, the District will consider factors that may heighten the risk of identity theft. Those factors include unauthorized access to a customer's account records or notification that a customer has provided fraudulent information. Appropriate responses may include the following:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords or other security devices that permit access to a covered account;
4. Not opening a new covered account;
5. Closing an existing covered account;
6. Notifying law enforcement; or
7. Determining that no response is warranted under the particular circumstances.

VI. Updating the Program

The District will update the Program periodically to reflect changes in risks to customers or to the integrity of the District's handling of covered accounts and/or changes to District offerings to customers regarding options for customer on-line access to covered accounts, such as:

1. The experiences of the District or customer with identity theft;
2. Changes in the methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts the District offers or maintains; and
5. Changes in the business arrangements of the District, including service provider arrangements.

VII. Methods for Administering the Program

While the CPNMD Board of Directors has reviewed and approved the Program and has ultimate responsibility for the Program, the Board designates the Assistant District Manager/Finance Manager as the "FACT Act Officer" responsible for the oversight, development, implementation and administration of the Program. The FACT Act Officer will provide annual reports to the Board demonstrating the Program's compliance. The CPNMD Board of Directors is responsible for reviewing the annual report and for approving material changes to the Program as necessary to address changing identity theft risks. The annual report will provide information as to the District's compliance with the FACT Act Red Flag rule and will address matters related to the Program such as:

1. Effectiveness of the District's policies and procedures addressing the risk of identity theft in connection with the opening of new accounts and with respect to the management of existing accounts;
2. Service provider arrangements, if any;
3. Significant incidents involving identity theft and management's response;
4. Recommendations for material changes to the Program, if any.

Any employee with access to the records of covered accounts will be trained to handle the covered accounts appropriately and identify Red Flags. Only employees with the consent of the FACT Act Officer will be granted access to open or close accounts or manage covered account record information. Some approved employees may be granted read-only access to covered accounts.

Should the District engage a service provider to perform an activity in connection with any covered accounts, the District will verify that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. An example of such a service provider would be any contractor or entity through which the District establishes the ability for customers to manage their accounts via electronic means, including access to account information and the ability to make payments electronically.

VIII. Additional Security Information

Although not required by the FACT Act, the District has adopted the following business practices to facilitate the prevention of identity theft:

1. Paper documents, files, and electronic media containing sensitive information are stored in secure areas;
2. Paper records containing sensitive information are shredded prior to being recycled;
3. Employees are alert to attempts at phone phishing;
4. Customer bank account information will be confirmed only if the customer provides the account information in question;
5. Anti-virus and anti-spyware programs are installed and run on District servers;
6. User names and passwords are required to access the billing system software;
7. Access to a customer's personal identifying information is limited to employees with a need to know;

8. Procedures exist to ensure that employees leaving employment with the District for any reason no longer have access to sensitive information;
9. No visitor is allowed unrestricted access to the District office or the District computer system.