RESOLUTION
OF THE BOARD OF DIRECTORS
OF BUCKHORN VALLEY METROPOLITAN DISTRICT NO. 2

A RESOLUTION ADOPTING AND APPROVING AN IDENTITY THEFT PREVENTION POLICY AND IDENTITY THEFT PREVENTION PROGRAM PROCEDURES

WHEREAS, the Buckhorn Valley Metropolitan District No. 2 (the "District") is a special district operating pursuant to Sections 32-1-101, *et seq.,* Colorado Revised Statutes; and

WHEREAS, the Federal Government has implemented new rules stemming from the Fair and Accurate Credit Transaction Act of 2003 (the "FACT Act"), 15 U.S.C. 1681 *et seq.*, to help consumers fight the growing crime of identity theft; and

WHEREAS, pursuant to Title 16, Chapter 1, part 681 of the Code of Federal Regulations (the "C.F.R."), a "creditor" that offers or maintains one or more covered accounts must develop and implement a written "Identity Theft Prevention Program" designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account; and

WHEREAS, pursuant to 15 U.S.C. 1691a(e), a "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

WHEREAS, pursuant to 16 C.F.R. § 681.2(b)(3), a "covered account" includes an account offered or maintained by the creditor primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, including, among other accounts, a credit card account, checking account, or savings account and any other account that the creditor offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks; and

WHEREAS, the District offers and/or maintains, or may in the future offer or maintain, covered accounts for services provided by the District in which the District extends, renews and/or continues credit to customers of the District for such services; and

WHEREAS, the Board of Directors of the Buckhorn Valley Metropolitan District No. 2 (the "Board") desires to adopt and approve an Identity Theft Prevention Program Policy and Identity Theft Prevention Program Procedures that are designed to detect, prevent, and mitigate identity theft in connection with covered accounts of customers of the District in compliance with the FACT Act.

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF THE DISTRICT THAT:

Section 1. Identity Theft Prevention Program Policy. The Board hereby adopts the following Identity Theft Prevention Program Policy to maintain maximum compliance with the FACT Act, its amendments, laws and regulations:

a. The Board hereby designates the _____ 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 Program including, but not limited to, adherence of the FACT Act and its implementing regulations.

b. The Board is 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 Program.

Section 2. FACT Act Identity Theft Prevention Program Procedures. To the extent the District offers or maintains covered accounts, the District shall comply with the following procedure. The Board hereby adopts the following FACT Act Identity Theft Prevention Program (the "Program") procedures, as may be amended from time to time by the Board:

a. Identifying Relevant Red Flags.

(1) *Risk Factors.* The District will consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(i) The types of covered accounts it offers or maintains;
(ii) The methods it provides to open its covered accounts:
(iii) The methods it provides to access its covered accounts; and
(iv) Its previous experiences with identity theft.

(2) *Sources of Red Flags.* The District will incorporate Red Flags from sources such as:

(i) Incidents of identity theft that the District has experienced;
(ii) Methods of identity theft that the District has identified that reflect changes in identity theft risks; and
(iii) Applicable supervisory guidance (i.e., state accounting and audit rules).

(3) *Categories of Red Flags.* The Program shall include relevant Red Flags from the following categories as appropriate. Examples of Red Flags from each of these categories are set forth in Paragraph 2.g. herein.

(i) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
(ii) The presentation of suspicious documents;
(iii) The presentation of suspicious personal identifying information, such as a suspicious address change;
(iv) The unusual use of, or other suspicious activity related to, a covered account; and
(v) 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.

b. Detecting Red Flags. The District will detect Red Flags in connection with the opening of new and existing accounts by:

(1) Obtaining identifying information about, and verifying the identity of, a person prior to opening an account, for example, using the policies and procedures, regarding identification and verification set forth in the District's rules, regulations and policies.

(2) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

c. Preventing and Mitigating Identity Theft. The District will document an appropriate response to each Red Flag that the District or customer has detected, commensurate with the degree of risk posed. In determining an appropriate response, the District will consider aggravating factors that may heighten the risk of identity theft such as a data security incident that results in unauthorized access to a covered account held by the District or third party, or notice that a customer has provided information related to a covered account held by the District to someone fraudulently claiming to represent the District or to a fraudulent website. Appropriate responses shall include the following:

(1) Monitoring a covered account for evidence of identity theft;

(2) Contacting the customer;

(3) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(4) Reopening a covered account with a new account number;

(5) Not opening a new covered account;

(6) Closing an existing covered account;

(7) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(8) Notifying law enforcement; or

(9) Determining that no response is warranted under the particular circumstances.

d. Updating the Program. The District will update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the District from identity theft, based on factors such as:

(1) The experiences of the District or customer with identity theft;

(2) Changes in methods of identity theft;

(3) Changes in methods to detect, prevent, and mitigate identity theft;

(4) Changes in the types of accounts that the District offers or maintains; and

(5) Changes in the business arrangement of the District, including service provider arrangements.

e. Methods for Administering the Program. The Board is ultimately responsible for the Program. However, the FACT Act Officer is responsible for the day-to-day administration and oversight. The FACT Act Officer is expected to:

(1) Assign specific responsibility for the Program's implementation;

(2) Review, prepare and provide, at least annually, reports to the Board on the District's compliance with the Program, the effectiveness of the policy and procedures, significant incidents involving identity theft and the District's response and recommendations for material changes to the Program;

(3) Obtain the Board's approval of changes to the procedures and policies if necessary to address changing identity theft risks; and

(4) Whenever the District engages a service provider to perform an activity in connection with one or more covered accounts, the FACT Act Officer will ensure 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. For example, the District should require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either

report the Red Flags to the District, or to take appropriate steps to prevent or mitigate identity theft.

f. Other Requirements. The District will be mindful of other related legal requirements that may be applicable, such as:

(1) Implementing any requirements regarding the circumstances under which credit may be extended when the District detects a fraud or active duty alert;

(2) Implementing any requirements for furnishers of information to consumer reporting agencies such as to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(3) Complying with the prohibitions on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

g. Identity Theft Prevention Program Red Flags. The District's Program will include, but not be limited to, the following Red Flags:

(1) Alerts, notifications or warnings from a consumer reporting agency such as:

(i) A fraud or active duty alert is included with a consumer report.
(ii) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
(iii) A consumer reporting agency provides a notice of address discrepancy.
(iv) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as: (1) a recent and significant increase in the volume of inquiries, (2) an unusual number of recently established credit relationships, (3) a material change in the use of credit, especially with respect to recently established credit relationships, or (4) an account that was closed for cause or identified for abuse of account privileges by the District.

(2) Suspicious documents including but not limited to:

(i) Documents provided for identification appear to have been altered or forged.
(ii) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

(iii) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

(iv) 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 a recent check.

(v) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

(3) Suspicious personal identifying information such as:

(i) Personal identifying information provided is inconsistent when compared against external information sources used by the District, such as the address does not match any address in the consumer report, or the social security number ("SSN") has not been issued, or is listed on the Social Security Administration's Death Master File.

(ii) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.

(iii) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the District, such as the address or phone number on the application is the same as the address or phone number provided on a fraudulent application.

(iv) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by third-party sources used by the District, such as the address on an application is fictitious, a mail drop, or a prison, or the phone number is invalid, or is associated with a pager or answering service.

(v) The SSN provided is the same as that submitted by other persons opening an account or other customers.

(vi) 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.

(vii) 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.

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

(ix) If the District uses challenge questions, 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.

(4) Unusual use of, or suspicious activity related to the covered account:

(i) Shortly following the notice of a change of address for a covered account, the District receives a request for the addition of authorized users on the account.

(ii) A new account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.

(iii) A covered account is used in a manner that is not consistent with established patterns of activity on the account, such as nonpayment where there is no history of late or missed payments or a material change in electronic fund transfer patterns in connection with a deposit account.

(iv) A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

(v) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

(vi) The District is notified that the customer is not receiving paper account statements.

(vii) The District is notified of unauthorized charges or transactions in connection with a customer's covered account.

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

ADOPTED AND APPROVED this 17th day of March, 2009.

BUCKHORN VALLEY METROPOLITAN
DISTRICT NO. 2 BOARD OF DIRECTORS

By: Samantha Gale
Its: Secretary/Treasurer

ATTEST:

By: Steve Kelly
Its: Director

M:\Buckhorn Valley Metro Nos. 1 & 2\Resolutions\2009
EDO1214
1150.0007