Resolution No. 2014-01-03

RESOLUTION
OF THE
BOARD OF DIRECTORS
OF THE
CASCADE METROPOLITAN DISTRICT NO. 1

Adopting an Identify Theft Prevention Program

WHEREAS, the Cascade Metropolitan District No. 1 (the "District") is a quasi-municipal corporation and political subdivision of the State of Colorado and a duly organized and existing special district pursuant to Title 32, Colorado Revised Statutes; and

WHEREAS, pursuant to federal law, the Federal Trade Commission adopted regulations requiring the creation of certain policies relating to the detection, prevention and mitigation of identity theft ("Identity Theft Rules"); and

WHEREAS, the Identity Theft Rules, adopted as 16 CFR § 681.1, require creditors, as defined by 15 U.S.C. § 1681a(r)(5), to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts; and

WHEREAS, 15 U.S.C. § 1691a defines a 'Creditor' as a person who regularly extends, renews or continues credit, and defines 'Credit' in part as 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 therefor; and

WHEREAS, the District is a creditor under the Identity Theft Rules by virtue of providing utility services or by otherwise accepting payment for services in arrears; and

WHEREAS, the Identity Theft Rules define "Covered Account" in part as an account that a creditor offers or maintains for personal, family or household purposes that involves or is designed to permit multiple payments or transactions, and specify that a utility account is a covered account; and

WHEREAS, the District provides water and wastewater services for which payment is made after the product is consumed or the service has otherwise been provided and, therefore, is subject to the Identity Theft Rules.

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

Section 1. Adoption of Identity Theft Prevention Program. The District hereby adopts the Identity Theft Prevention Program set forth in **Exhibit A**, attached hereto and incorporated herein.

Section 2. Preambles Incorporated. The preambles to this Resolution are hereby incorporated into this Resolution as if set out fully herein.

Section 3. Severability. If any part, section, subsection, sentence, clause or phrase of this Resolution is for any reason held to be invalid, such invalidity shall not affect the validity of the remaining provisions.

Section 4. Effective Date. This Resolution shall become effective as of January 18, 2014, shall be enforced immediately thereafter and shall supersede any previous policy related to identity theft. This Resolution shall be implemented and administered by the District to conform with all requirements of the Identity Theft Rules, as modified from time to time.

[Remainder of Page Intentionally Left Blank].

RESOLVED AND ADOPTED this 18th day of January 2014.

CASCADE METROPOLITAN DISTRICT NO. 1, a quasi municipal corporation and political subdivision of the State of Colorado

By: _____
Officer of the District

ATTEST:

_____

APPROVED AS TO FORM:
WHITE, BEAR & ANKELE,
Professional Corporation

_____
General Counsel to the District

[Signature Page to Identity Theft Prevention Program Resolution]

EXHIBIT A

IDENTITY THEFT PREVENTION PROGRAM

The purpose of the Identity Theft Prevention Program is to comply with 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and responding to such red flags in a manner that will prevent identity theft.

Section 1. Definitions. For purposes of this Program, the following definitions apply to the following terms, whether or not capitalized herein:

(1) "Covered account" means:

(a) an account that the District offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a utility account; and

(b) any other account that the District offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the District from identity theft including financial, operational, compliance, reputation, or litigation risks.

(2) "Credit" means the right granted by the District 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 therefor.

(3) "Creditor" means the District.

(4) "Customer" means a person that has a covered account with the District.

(5) "District" means the Cascade Metropolitan District No. 1.

(6) "Identity theft" means a fraud committed or attempted using identifying information of another person without authority.

(7) "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(8) "Personal Identifying Information" means a person's credit card account information, debit card information, bank account information and drivers' license information and for a natural person includes their social security number, mother's birth. name, and date of birth.

(9) "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) "Service provider" means a person that provides a service directly to the District.

Section 2. Findings

(1) The District 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 District services include water and wastewater services.

(3) The District's previous experience with identity theft related to covered accounts is as follows:

(a) None.

(4) The processes of opening a new covered account, restoring an existing covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur.

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

(6) The District determines that there is a low risk of identity theft to its customers occurring in the following ways (if any):

(a) Use by an applicant of another person's personal identifying information to establish a new covered account.

(b) Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name.

(c) 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.

(d) Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account, or other method of payment.

Section 3. Process of Establishing a Covered Account

(1) Accounts are opened by the District after notification provided by a title company and/or customer. Account balances follow the property not the customer, and no additional identifying information for the customer is requested by the District.

(2) Each account shall be assigned a customer account number which shall be unique to that account. The District may utilize computer software to encrypt account numbers and PINs.

Section 4. Access to Covered Account Information

(1) Access to customer accounts shall be password protected and shall be limited to authorized personnel of the District.

(2) Such password(s) shall be changed by the manager of the department providing the service for which the covered account is created on a regular basis. Passwords shall be at least 8 characters in length and shall contain letters, numbers and symbols.

(3) Any unauthorized access to or other breach of customer accounts is to be reported immediately to the District Manager and the password changed immediately.

(4) Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the District Manager.

Section 5. 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 District's website shall be entered directly into the customer's account information in the computer data base. Immediately upon processing of the credit card, any information referencing the credit card is immediately shredded by the District.

(3) Customer account statements and receipts for covered accounts shall include only the last four digits of the credit or debit card or the bank account used for payment of the covered account.

Section 6. Sources and Types of Red Flags

All employees responsible for or involved in the process of opening a covered account, restoring a covered account, or accepting payment for a covered account, shall check for red flags as indicators of possible identity theft. Such red flags include:

(1) Suspicious documents. Examples of suspicious documents include, but are not limited to:

(a) Documents provided for identification that appears to be altered or forged;

(b) Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;

(c) Identification on which the information is inconsistent with information provided by the applicant or customer;

(d) Identification on which the information is inconsistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check; or

(e) An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

(3) Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:

(a) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer;

(b) Personal identifying information or a phone number or address is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the District;

(c) Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity;

(d) 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 applicants or customers;

(e) The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;

(f) Personal identifying information is not consistent with personal identifying information that is on file with the District; or

(g) The applicant or 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 relating to a covered account. Examples of suspicious activity include:

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

(b) A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

(i) The customer fails to make the first payment or makes an initial payment but no subsequent payments.

(c) An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

(i) Nonpayment when there is no history of late or missed payments; or

(ii) A material change in purchasing or spending patterns.

(d) An account that has been inactive for a long period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);

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

(f) The District is notified that the customer is not receiving paper account statements;

(g) The District is notified of unauthorized charges or transactions in connection with a customer's account; or

(h) The District is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

(5) Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

Section 7. Prevention and Mitigation of Identity Theft.

(1) In the event that any employee responsible for or involved in restoring an ***existing*** covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the District Manager. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the District Manager, who may in his or her discretion determine that

no further action is necessary. If the District Manager in his or her discretion determines that further action is necessary, an employee of the District shall perform one or more of the following responses, as determined to be appropriate by the District Manager:

(a) Contact the customer;

(b) Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:

(i) Change any account numbers, passwords, security codes, or other security devices that permit access to an account; or

(ii) Close the account.

(c) Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;

(d) Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or

(e) Take other appropriate action to prevent or mitigate identity theft.

(2) In the event that any employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the District Manager. If; in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the District Manager, who may in his or her discretion determine that no further action is necessary. If the District Manager in his or her discretion determines that further action is necessary, an employee of the District shall perform one or more of the following responses, as determined to be appropriate by the District Manager:

(a) Request additional identifying information from the applicant;

(b) Deny the application for the new account;

(c) Notify law enforcement of possible identity theft; or

(d) Take other appropriate action to prevent or mitigate identity theft.

Section 8. Updating the Program

The Board of Directors shall annually review and, based upon recommendations of District Counsel and the District Manager, update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the District and its covered accounts from identity theft. In so doing, the Board shall consider the following factors and exercise its discretion in amending the program:

(a) The District's experiences with identity theft;

(b) Updates in methods of identity theft;

(c) Updates in customary methods used to detect, prevent, and mitigate identity theft;

(d) Updates in the types of accounts that the District offers or maintains; and

(e) Updates in service provider arrangements.

Section 9. Program Administration

The District's Senior Level Staff in charge of billing is responsible for oversight of the program and for program implementation. The District Manager is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the District Manager, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program shall be submitted to the Board of Directors for consideration by the Board.

(a) The Senior Level Staff will report to the District Manager at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:

(i) The effectiveness of the policies and procedures of the District in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

(ii) Service provider arrangements;

(iii) Significant incidents involving identity theft and management's response; and

(iv) Recommendations for material changes to the Program.

(2) The Senior Level Staff is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing covered account or accepting payment for a covered account with respect to the implementation and requirements of the identity Theft Prevention Program. The Senior Level Staff shall exercise his or her discretion in determining the amount and substance of training necessary.

Section 10. Outside Service Providers

In the event that the District engages a service provider to perform an activity in connection with one or more covered accounts, the Senior Level Staff 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 any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.