RESOLUTION NO. 2009-02

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE RANCHO MURIETA COMMUNITY SERVICES DISTRICT ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM PURSUANT TO THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT AND THE FEDERAL TRADE COMMISSION'S RED FLAG RULES

WHEREAS, the Federal Trade Commission (FTC) and other federal regulatory agencies have recently published rules and guidelines for regulating identity theft; and

WHEREAS, the new regulations implement the Fair and Accurate Credit Transactions Act of 2003 (FACTA), 15 U.S.C. sections 1681 *et seq.*; and

WHEREAS, the FTC's regulations are known as the "Red Flag Rules" (Rules), 16 C.F.R. Part 681; and

WHEREAS, the Rules require "creditors" that maintain "covered accounts" to develop and implement an identity theft prevention program; and

WHEREAS, local governmental entities are considered to be "creditors" if the entity provides goods or services for which payment by the customer is deferred; and

WHEREAS, local governmental entities maintain "covered accounts" if the entity maintains (1) accounts designed to permit multiple payments or transactions, such as utility accounts, or (2) other accounts where there is a continuing relationship between the entity and customer and a reasonably foreseeable risk to customers or entity of identity theft exists; and

WHEREAS, the Rules require creditors that maintain covered accounts to 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, the identity theft prevention program must be appropriate to the size and complexity of the creditor and the nature and scope of its activities; and

WHEREAS, the Rancho Murieta Community Services District (District) is a "creditor" that maintains "covered accounts" because the District provides water, sewer, drainage, security and solid waste service(s) to customers and maintains covered accounts for such customers; and

WHEREAS, the District desires to adopt an identity theft prevention program in compliance with the Rules to detect, prevent and mitigate identity theft in connection with the water, sewer, drainage, security and solid waste services it provides and the customer accounts it maintains for these services.

NOW, THEREFORE, the Board of Directors of Rancho Murieta Community Services District does hereby find, determine and resolve as follows:

1. The Identity Theft Prevention Program (Program), attached as Exhibit A and incorporated herein by reference, has been developed in compliance with FACTA the Rules.

2. The Program is appropriate to the size and complexity of the District and the nature and scope of its activities.

3. The Program is hereby approved and adopted.

4. The Program shall be immediately implemented by the Director of Administration.

PASSED AND ADOPTED this 20th day of May, 2009 by the following roll call vote:

AYES: Belton, Kjome, Ferraro, Mobley, Taylor
NOES: None
ABSTAIN: None
ABSENT: None

Roberta Belton, President of the Board
Rancho Murieta Community Services District

ATTEST:

Suzanne Lindenfeld, District Secretary

Exhibit A

Rancho Murieta Community Services District
Identity Theft Prevention Program

I. PROGRAM INTRODUCTION

This Identity Theft Prevention Program (Program) is developed and implemented pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA), 15 U.S.C. 1681 *et seq.*, and regulations of the Federal Trade Commission (FTC) known as the "Red Flag Rules" (Rules), 16. C.F.R. Part 681 that were designed and adopted in compliance with FACTA. The Rules require the Rancho Murieta Community Services District (District) to develop and implement a program to detect, prevent and mitigate identity theft. This Program is intended to memorialize and outline the identity protections and procedures of the District and to formalize their continued use and update, as required by law.

II. PROGRAM PURPOSE

A. The District places the highest priority on protecting any confidential financial and personal information submitted to it in the course of providing District services. This Program applies to the water, sewer, drainage, security and solid waste services offered and maintained by the District.

B. This Program has the following purposes:

1. Identify "red flags" applicable to the accounts offered and maintained by the District and incorporate those "red flags" into this Program.

2. Detect those "red flags" that have been incorporated into this Program as they occur.

3. Ensure that staff responds appropriately to detected "red flags" so as to prevent and mitigate identity theft.

4. Ensure that this Program is updated periodically to reflect changes in identity theft risk to District customers or to the District.

5. Ensure that all service providers' activities are conducted in accordance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft.

III. DEFINITIONS

A. For purposes of this Program, the words set forth below shall have the following meanings:

1. "Account" means the water, sewer, drainage, security and garbage services offered and maintained by the District. These accounts qualify as "accounts" and "covered accounts" as defined by the Rules under 16 C.F.R. section 681.2.

2. "Customer" means a person that is identified as the property owner on the county's recorded deed of ownership for properties within the District.

3. "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 any:

   (a) Name, Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; unique electronic identification number, address, or routing code, or as otherwise provided in 16 C.F.R. section 603.2.

4. "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority or as otherwise provided in 16 C.F.R. section 603.2.

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

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

7. "Service provider" means a person that provides a service directly to the District in connection with one or more accounts.

8. "Staff" means the District staff that has access to identifying information of Customers during the opening and maintaining of the accounts.

IV. IDENTIFICATION OF RED FLAGS

A. The District has completed an assessment of the accounts it offers and maintains to determine potential red flags that may arise in connection to the accounts. The District has assessed the following: (1) the type(s) of accounts offered and maintained by the District; (2) the methods the District uses to open accounts; (3) the methods it provides to allow staff and customers to access accounts; and (4) the District previous experiences with identity theft.

B. Based on the foregoing assessment, the District has determined that the existence of any of the following red flags in connection with any account indicates the possible existence of identity theft:

   1. **Suspicious Customer Identifying Information**

      (a) The identifying information provided by the customer is inconsistent when compared against external information sources used by the District. For example:

         (i) Information provided by the customer is inconsistent with District records.

      (b) The identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer.

(c) The identifying information provided by the customer is associated with known fraudulent activity as indicated by internal or third-party sources used by the District.

(d) The identifying information provided by the customer is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the District.

(e) The customer identifying information is not consistent with identifying information that is on file with the District.

(f) A customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report. For example, the customer cannot answer a challenge question.

2. **Suspicious Activity**

(a) Shortly following receipt of a notice of a change of address from a customer for their account, the District receives additional requests for changes to the account.

(b) An account is used in a manner that is not consistent with established patterns of activity on the account. For example, the customer misses a payment when there is no history of late or missed payments.

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

(d) The District is notified that the customer is not receiving paper account statements or billing statements.

(e) The District is notified of unauthorized transactions in connection with a customer's account.

3. **Notices From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other persons**

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

V. DETECTION OF RED FLAGS

A. In connection with the opening and maintaining of any account, staff shall take the steps set forth below to detect red flags.

B. **Opening New Accounts:**

1. New accounts are opened upon receipt of recorded grant deeds or other formal notice of ownership change and receipt of the transfer fee.

2. Staff shall obtain the following identifying information to verify the identity of each customer: recorded county deed of ownership.

3. Staff shall review the obtained identifying information for any red flags identified in Section IV of this Program.

4. Staff shall verify the customer's identity through the comparison of the identifying information and any other information provided by the customer with information contained in District files, or information obtained from any other source.

5. If the customer is not an individual and staff cannot verify the customer's identity through the steps listed above, staff may, based on a risk assessment, obtain identifying information of and verify the identity of the individuals with authority or control over the account, including signatories, pursuant to the steps listed above.

C. **Maintaining Existing Accounts:**

1. Staff shall verify the identity of each customer that requests account information, other than a request for the outstanding balance owed, to the extent reasonable and practicable. The name, credit history, utility usage data, home address, or telephone number of a customer shall not be provided to any person that is not verified to be the customer, except to the extent required by California Government Code section 6254.16.

2. Staff shall reasonably monitor the transactions of the accounts maintained by the District for any red flags identified in Section IV of this Program.

3. Staff shall verify the validity of any notice of change of address or notice of change of billing information by contacting the customer and/or through the comparison of the identifying information in the notice of change of address or notice of change of billing information and any other information provided by the customer with information contained in District files, or information obtained from any other source.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

A. In the event that staff detects any red flags related to an account, staff shall respond to the red flag by taking one or more of the responsive actions set forth below. In responding to a red flag, staff shall take into consideration which actions are appropriate for the degree of risk of identity theft posed by the red flag.

B. **Responses to Detected Red Flags**

1. Contact the customer.

2. Reopen an account with a new account number.

3. Refuse to open a new account.

4. Notify law enforcement and/or prosecutorial agencies.

5. Determine that no response is warranted under the particular circumstances.

6. Notify the Director of Administration for determination of the appropriate step(s) to take.

C. Each situation shall be evaluated on a case-by-case basis. In determining an appropriate response, staff shall consider any aggravating factors that may heighten the risk of identity theft. For example, a data security incident that results in unauthorized access to a customer's account records held by the District, receipt of notice that a data security incident has occurred that results in unauthorized access to a customer's account records held by a third-party, or receipt of notice that a customer has provided information relating to an account with the District to someone fraudulently claiming to represent the District or to a fraudulent website.

VII. ADMINISTRATION AND UPDATING OF THIS PROGRAM

A. This Program shall be administered by the Director of Administration.

1. The Director of Administration shall be responsible for:

(a) Assigning the specific responsibility for this Program's implementation to the appropriate staff.

(b) Reviewing annual reports prepared by staff regarding compliance by the District with FACTA and the Rules.

(c) Approving material changes to this Program as necessary to address changing identity theft risks.

B. **Annual Reports**

1. Staff shall provide annual reports to the Director of Administration regarding compliance of this Program with the Rules.

2. The annual reports shall address any material matters related to this Program and evaluate any issues related to this Program, including:

(a) The effectiveness of this Program in addressing the risk of identity theft in connection with the opening and maintaining of accounts.

(b) Any arrangements with new service providers or any changes in the arrangements with existing service providers to detect, prevent and mitigate identity theft, if applicable.

(c) Any significant incidents involving identity theft and staff's response to those incidents.

(d) Changes in methods of identity theft.

(e) Changes in methods to detect, prevent and mitigate identity theft.

(f) Changes in the types of accounts the District offers or maintains.

(g) Recommendations for material changes to this Program.

C. **Updating this Program**

1. Upon review of the annual reports submitted by staff and the recommendations contained therein, the Director of Administration shall determine whether material changes to this Program are necessary to update this Program to better detect, prevent and mitigate identity theft related to the accounts offered and maintained by the District.

2. If the Director of Administration determines that such an update to this Program is necessary, the Director of Administration shall direct staff to draft the recommended material change(s) to this Program, which shall be submitted to the Director of Administration for approval.

D. **Staff Training**

1. The Director of Administration shall ensure that Staff is trained as necessary to effectively implement this Program, which includes training regarding any approved material changes to this Program.

VIII. OVERSIGHT OF SERVICE PROVIDERS

A. The District shall take steps necessary to ensure that the activity of any service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

B. The Director of Administration shall determine which steps are necessary to ensure the activities of any service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. The Director of Administration may, if he or she deems it appropriate, require a service provider by contract to design and implement policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities related to the accounts, and either report the red flags to the Director of Administration or to take appropriate steps to prevent or mitigate identity theft.