SWEETWATER SPRINGS WATER DISTRICT

TO: Board of Directors **AGENDA NO. III-E**

FROM: Steve Mack, General Manager

Meeting Date: **May 7, 2009**

Subject: **Identity Theft Prevention Program**

RECOMMENDED ACTION:

Adopt Ordinance 38, Adding Policy Number 3140 to the District's Policy and Procedures, Identity Theft Prevention Program.

FISCAL IMPACT:

Minimal.

DISCUSSION:

Ordinance 38 was introduced at the April meeting, and at that same meeting Resolution 09-11 of the same title and content was approved so that that the Identity Theft Prevention Program could be implemented immediately.

ORDINANCE 38

AN ORDINANCE OF SWEETWATER SPRINGS WATER DISTRICT ADDING POLICY NUMBER 3140 TO THE DISTRICT'S POLICY AND PROCEDURES, IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Board wishes to be in compliance with the Federal Trade Commission's (FTC) Fair and Accurate Credit Transactions Act; and

WHEREAS, the Board is desirous of protecting confidential customer information; and

WHEREAS, the Board is not aware of previous incidences of consumer identity theft at the District or other misuse of confidential customer information that is maintained by the District; and

WHEREAS, the Board nonetheless desires to ensure that new water accounts are legitimate and the information collected to open the accounts is useful to the District and does not pose an unnecessary risk of identity theft for the customer; and

WHEREAS, suggested "Red Flags" for identity theft have been reviewed for applicability to the Sweetwater Springs Water District operations; and

WHEREAS, the Board is aware that certain consumer information is collected from customers to help the Collections Agency track down delinquent customers; and

WHEREAS, the Collections Agency will continue to track down delinquent customers even if it does not have all the consumer information the District currently collects; and

WHEREAS, the Board is aware that the District's share of funds actually collected by the Collection Agency totaled $797.89 in FY 2007-08 compared to $1.92 million in water sales; and

WHEREAS, the Board wishes for the Identity Theft Prevention Policy become a part of the District's Policies and Procedures by ordinance.

NOW THEREFORE BE IT ORDAINED by the Board of Directors of the Sweetwater Springs Water District, County of Sonoma, as follows:

Section 1. Policy Number 3140 of the Sweetwater Springs Water District Policy & Procedures, is hereby **added** as follows.

Policy Title: **Identity Theft Prevention Program**
Policy Number: 3140

3140.10 Introduction. This program has been implemented to comply with the Federal Trade Commissions (FTC) Fair and Accurate Credit Transactions Act ("Red Flag Rule"). The primary purpose of the Red Flag Rule is to detect and protect against identity theft and the establishment of false accounts, and to ensure that existing accounts are not being manipulated. In addition, the Sweetwater Springs Water District is interested in protecting customer information.

The Office Manager will be responsible for this program.

3140.15 Risk Assessment, Training and Policy Review. As part of the Risk Assessment required by the Red Flag Rule, the following Red Flags were reviewed to assist in determining which red flags are applicable to and should be adopted by the Sweetwater Springs Water District:

- Documents provided by the customer for identification appear to have been altered or forged
- The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification
- Other information on the identification is not consistent with information provided by the customer
- 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
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- The identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the Social Security Number range and date of birth.
- 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. For example, the address or phone number on an application is the same as the address or phone number provided on a fraudulent application.
- 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, such as a prison mailing address or an invalid phone number.

- The Social Security Number provided by the customer is the same as that submitted by other customers opening accounts or having existing accounts with the District.
- The address or telephone number provided by the customer is the same as or similar to the address or telephone number submitted by an unusually large number of other customers opening accounts or having existing accounts with the District.
- A customer opening an account or having an existing account fails to provide all required identifying information on an application or in response to notification that the application is incomplete.
- The customer identifying information is not consistent with identifying information that is on file with the District.
- A customer opening an account or having an existing account 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.
- 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.
- 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.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
- The District is notified that the customer is not receiving paper account statements or billing statements.
- The District is notified of unauthorized transactions in connection with a customer's account.
- 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.

The Identity Theft Prevention Policy and listed Red Flags will be reviewed with staff on an annual basis to ensure adequate training of staff and adequacy of the Policy.

3140.20 <u>False/Fraudulent Accounts.</u>

3140.21 Procedures to protect against false/fraudulent accounts. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary

1. Red Flag: No mailing address. Do not open accounts for customers who cannot provide a mailing address.

2. Red Flag: No telephone number. Ask for telephone number. Many customers do not have telephone numbers, so lack of one will not stop an account from being opened, but it is a Red Flag that can be considered in conjunction with other suspicious items.

3. Red Flag: Employment. Ask for name of employer and telephone number at work. Lack of information on employment will not stop an account from being opened but it's a Red Flag that can be considered in conjunction with other suspicious items.

3. Red Flag: No tenancy agreement. Accounts opened for customers who cannot provide proof of tenancy shall be closed in a short period of time. If customer fails to provide proof of tenancy within 5 days of opening the account, the account shall be posted with a Turn Off Notice, then closed.

4. Red Flag: Proof of ownership. For accounts that are owner-occupied, staff will reconcile ownership records with County ownership records when assessments are reported.

5. Red Flag: Accounts opened over the phone. Most accounts are opened over the phone and District staff do not see new account holders in person. The information collected over the phone will be examined with the Red Flags of Section 3140.15 in mind and suspicious accounts will have staff followup.

5. Red flag: General suspicion of fraud. Discuss and follow up on suspicious phone conversations, in-office conversations, or other circumstances that are similar to those listed in above in Section 3140.15.

3140.30 Protection of Customer Information

3140.31 Procedures to protect customer information

1. Red Flag: Theft of information. Lock tags and tagbooks up at the end of the work day rather than leaving them on desktops.

Store dated information in the vault. Destroy (versus throwing in the garbage or recycle bin) records not required to be kept.

2. Red Flag: Highly confidential information. Discontinue collecting the full social security number and driver's license of customers. Collect only the last four digits of the social security number.

3. Red Flag: Existing confidential information. Paper records containing confidential information will be shredded on current destruction schedule and kept in locked storage. Computer records containing SSN and driver's license number will have that information deleted to conform with 3140.31.2 above.

Section 2. Severance Clause. If any section, subsection, sentence, clause or phrase or word of this ordinance is for any reason held to be unconstitutional, unlawful or otherwise invalid by a court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this ordinance. The Board of Directors hereby declares that it would have passed and adopted this ordinance and each and all provisions thereof irrespective of the fact that any one or more of said provisions be declared unconstitutional, unlawful or otherwise invalid.

Section 3. Effective Date.
This ordinance shall become effective thirty (30) days after the date of its adoption by the Board of Directors.

This Ordinance was adopted this 7th day of May, 2009, on roll call by the following vote:

Jim Quigley _____
Gaylord Schaap: _____
Victoria Wikle: _____
Wanda Smith: _____
Ken McLean : _____

_____
Victoria Wikle
President of the Board

ATTEST:

_____
Julie A. Kenny
Clerk of the Board