NAPA-VALLEJO WASTE MANAGEMENT AUTHORITY

Agenda Date: 4/2/2009
Agenda Placement: 6C

Napa-Vallejo Waste Management Authority
Board Agenda Letter

TO:	Board of Directors
FROM:	Trent Cave - Manager Napa-Vallejo Waste Management Authority
REPORT BY:	Susan Altman, ATTORNEY II - 707-299-1479
SUBJECT:	Resolution Adopting Identity Theft Protocols

RECOMMENDATION

RESOLUTION TO ADOPT IDENTITY THEFT PROTOCOLS
REQUESTED ACTION: Approval of Resolution #09-04 adopting an Identity Theft Prevention Program.

EXECUTIVE SUMMARY

Adoption of this Resolution will be the first step in implementing an Identity Theft Prevention Program as required by the Federal Trade Commission (FTC) regulations adopted in 2003. Counsel has recommended placement of this item on the April 5 agenda in order to meet the May 1 adoption and implementation requirements outlined in the Resolution.

FISCAL IMPACT

Is there a Fiscal Impact? No

ENVIRONMENTAL IMPACT

ENVIRONMENTAL DETERMINATION: The proposed action is not a project as defined by 14 California Code of Regulations 15378 (State CEQA Guidelines) and therefore CEQA is not applicable.

BACKGROUND AND DISCUSSION

Adoption of this Resolution will be the first step in implementing an Identity Theft Prevention Program for the Authority as required by the Federal Trade Commission (FTC) regulations adopted in 2003. Counsel has recommended placement of this item on the April 5 agenda in order to meet the May 1 adoption and implementation requirements stated in the Resolution. Staff intends to piggyback on Napa County's training session in order to gain a full understanding of the requirements for complying with and fully implementing this Program. The following Red Flags Rule explanation was provided to Authority staff by Counsel.

The Red Flags Rule (hereinafter "Rules") are federal regulations enacted as part of the Fair and Accurate Transactions Act of 2003 to reduce identity theft by requiring public and private entities to implement policies and procedures to identify and prevent identity theft. The Rules require financial institutions and creditors to develop and implement written identity theft prevention programs by May 1, 2009 (this date was extended from November 1, 2008).

Among others, the Rules apply to (1) "creditors" with "covered accounts. Under the Acts, Creditors include government entities who defer payment for goods or services (i.e. payment for utilities). Deferring payments refers to postponing payments to a future date and/or installment payments on fines or costs. And a covered account is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions or any other account for which there is a foreseeable risk to customers or safety and soundness of the financial institution or creditor from identity theft. Covered accounts include, but are not limited to, cell phone accounts, checking accounts, saving accounts, and utility accounts.

A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. Red Flags fall into five categories: (1) alerts, notifications, or warnings from a consumer reporting agency; (2) suspicious documents; (3) suspicious personal identification information, such as a suspicious address; (4) unusual or suspicious activity relating to a covered account; and (5) notices from consumers, victims of identity theft, law enforcement, or other businesses regarding possible identity theft in connection with covered accounts

The Rules provide that financial institutions and creditors must design a program that can detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be managed by the Board of Directors or senior employees of the creditor, include appropriate staff training, and provide for oversight of any service providers. The program must contain reasonable policies and procedures and contain four basic elements: (1) identify relevant Red Flags for covered accounts and incorporate those Red Flags into the program; (2) detect Red Flags that have been incorporated into the program; (3) respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and (4) ensure the program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

SUPPORTING DOCUMENTS

A . Resolution 09-04

Manager: Approve

Reviewed By: Martha Burdick