COUNTY OF TULARE
OFFICE OF THE COUNTY ADMINISTRATOR

ADMINISTRATIVE REGULATION NO. 36
(Resolution No. 2009-0302)

SUBJECT: IDENTITY THEFT "RED FLAG" PREVENTION PROGRAM POLICY

EFFECTIVE DATE: 5-01-09

REVIEWED: March 16, 2009

Purpose

The Federal Trade Commission has issued regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs by May 1, 2009. The Fair and Accurate Credit Transactions (FACT) Act of 2003, requires the implementation of an identity theft prevention program designed to identify, detect, and respond to patterns, practices, or specific activities that could indicate that identity theft has taken place against a County of Tulare (County) customer. The primary purpose of the rule is the protect against the establishment of false accounts and ensure existing accounts are not being manipulated.

Background

Pursuant to the Federal Trade Commission's Red Flags Rule, this policy implements Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2003 and 16 Code of Federal Regulations (CFR) § 681.2. The FACT Act is enacted to curtail the effects of identity theft. The FACT Act has been amended to require that all creditors (which could include local government) establish policies and procedures to help prevent identity theft. The Code of Federal Regulation provides specific examples of indicators of possible identity theft. Attached as Appendix A is a list of other security procedures a department may consider to protect consumer information and to prevent unauthorized access.

Definitions

A. "Account" means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account Includes:
   (i) An extension of credit, such as the purchase of property or services involving a deferred payment; and
   (ii) A deposit account.

B. **"**Covered account**"** means an account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes, and that involves multiple payments or transactions. Covered accounts also include an account that a creditor offers or maintains for which there is a foreseeable risk to

customers or the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risk.

C. "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. Where a government entity (e.g. County) defers payments for goods or services, they, too, are to be considered creditors (for example, payment plans for parking tickets).

D. "Credit" means 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.

D. "Customer" means a person that has a covered account with a creditor (County).

E. "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: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

F. "Identity theft" means fraud committed using the identifying information of another person.

G. "Payment deferral" means postponing payments to a future date and/or installment payments on fines or costs.

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

Program Policy and Procedure

The County will act to identify, detect, and respond to patterns, practices, or specific activities that could indicate that identity theft has taken place against a County customer. County Departments who are considered "creditors" with "covered accounts" are required to establish an identity theft prevention program *tailored to its size*, *complexity* and the *nature of its operations*. In order to do this County staff will prepare reasonable policies and procedures which include but are not limited to:

A. **IDENTIFICATION OF RED FLAGS**.

Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into County procedures. In order to identify relevant

Red Flags, the County shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and its previous experience with Identity Theft. The County identifies the following Red Flags, in each of the listed categories:

1. Notification and Warnings From Credit Reporting Agencies

   Red Flags

   a. Report of fraud accompanying a credit report;
   b. Notice or report from a credit agency of a credit freeze on a customer or applicant;
   c. Notice or report from a credit agency of an active duty alert for an applicant; and
   d. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

2. Suspicious Documents

   Red Flags

   a. Identification document or card that appears to be forged, altered or inauthentic;
   b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
   c. Other document with information that is inconsistent with existing customer information (such as a person's signature on a check appears forged); and
   d. Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information

   Red Flags

   a. Identifying information presented that is inconsistent with other information the customer provides (such as inconsistent birth dates);
   b. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a driver's license);
   c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

d. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
e. Social security number presented that is the same as one given by another customer;
f. An address or phone number presented that is the same as that of another person;
g. Failing to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
h. Identifying information which is not consistent with the information that is on file for the customer.

4. Suspicious Account Activity or Unusual Use of Account

Red Flags

a. Change of address for an account followed by a request to change the account holder's name;
b. Payments stop on an otherwise consistently up-to-date account;
c. Account used in a way that is not consistent with prior use (such as very high activity);
d. Mail sent to the account holder is repeatedly returned as undeliverable;
e. Notice to the County that a customer is not receiving mail sent by the County;
f. Notice to the County that an account has unauthorized activity;
g. Breach in the County's computer system security;
h. Unauthorized access to or use of customer account information.

5. Alerts from Others

Red Flags

a. Notice to the County from a customer, a victim of identity theft, a law enforcement authority or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

B. DETECTING RED FLAGS

Detect Red Flags that have unintentionally been incorporated into a County program, which shall include New Accounts and Existing Accounts.

1. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account; County staff shall take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

a. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
b. Verify the customer's identity (for instance, review a driver's license or other identification card);
c. Review documentation showing the existence of a business entity; and
d. Independently contact the customer.

2. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, County staff will take the following steps to monitor transactions with an account:

Detect Red Flags

a. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
b. Verify the validity of requests to change billing addresses; and
c. Verify changes in banking information given for billing and payment purposes.

C. PREVENTING AND MITIGATING IDENTITY THEFT

Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.

1. Prevent and Mitigate Identity Theft

In the event County staff detects any identified Red Flags, such staff shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

a. Monitor a covered account for evidence of Identity Theft;
b. Contact the customer with the covered account;
c. Change any passwords or other security codes and devices that permit access to a covered account;
d. Not open a new covered account;

e. Close an existing covered account;
f. Reopen a covered account with a new number;
g. Not attempt to collect payment on a covered account;
h. Notify the Program Administrator for determination of the appropriate step(s) to take;
i. Notify law enforcement; or
j. Determine that no response is warranted under the particular circumstances.

2. Protect Customer Identifying Information

In order to further prevent the likelihood of Identity theft occurring with respect to County accounts, the County shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

a. Secure the County website but provide clear notice that the website is not secure;
b. Undertake complete and secure destruction of paper documents and computer files containing customer information;
c. Make office computers password protected and provide that computer screens lock after a set period of time;
d. Keep offices clear of papers containing customer identifying information;
e. Request only the last 4 digits of social security numbers (if any);
f. Maintain computer virus protection up to date; and
g. Require and keep only the kinds of customer information that are necessary for County purposes.

D. PROGRAM UPDATES

Ensure that County procedures are updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft.

Program Policy and Procedure Updates

The County Program Policy and Procedure will be periodically reviewed to reflect changes in identity theft risks to County customers and to the safety and soundness of the County program from identity theft. At least annually, the Program Administrator shall consider the County's experiences with identity theft, changes in identity Theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the County maintains and changes in the County's business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall

determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall update and implement the revised Program and present the Program Administrator's recommended changes to the Board of Supervisors for review and approval.

Program Administration

A. **Oversight**

Responsibility for developing, implementing and updating this administrative regulation lies with the County Administrative Office. County Departments affected by the FACT Act shall appoint a Program Administrator who will be responsible for developing, implementing and updating departmental programs and procedures. The departmental Program Administrator will be responsible for the administration of policy and procedure, for ensuring appropriate training of County staff on the policy and procedure, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the policy and procedure.

B. **Staff Training and Reports**

County staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. The Program Administrator may include in its Program how often training is to occur. The Program Administrator may also require staff to provide reports to the Program Administrator on incidents of identity theft, the department's compliance with the Program and the effectiveness of the Program.

C. **Service Provider Arrangements**

In the event the County engages a service provider to perform an activity in connection with one or more covered accounts, the County shall take the following steps to require that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

1. Require, by contract, that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to County covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program; or

2. Require, by contract, that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to County covered accounts in compliance with the terms and conditions of the service provider's identity theft prevention program and will take appropriate action to prevent and mitigate identity theft; and that the service providers agree to report promptly to the County in writing if the service provider in connection with a County covered account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.

D. Customer Identification Information and Public Disclosure

The identifying information of County customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law. The County Board of Supervisors also finds and determines that public disclosure of the County's specific practices to identify, detect, prevent and mitigate identity theft may compromise the effectiveness of such practices and hereby directs that, under the Program, knowledge of such specific practices shall be limited to the Program Administrator and those County employees and service providers who need to be aware of such practices for the purpose of preventing Identity theft.

E. Identity Theft Prevention Program Review and Approval

This Identity Theft Prevention Program has been reviewed and adopted by the Tulare County Board of Supervisors who will allow each department to designate senior management in the oversight, development, implementation and administration of the Program.

The Program Administrator:_____

Position:_____

Date:_____

Signature:_____

The following staff has been trained on the contents and procedures of this Program.

Signatures:

1._____

2._____

3._____

4._____

A report will be prepared annually and submitted to the above named Program Administrator or governing body to include matter related to the program, the effectiveness of the policies and procedures, and a summary of any identity theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.