MEMORANDUM

OFFICE OF THE

COUNTY EXECUTIVE OFFICE

COUNTY OF PLACER

TO: Honorable Board of Supervisors

FROM: David Boesch, County Executive Officer
By: Denise Medlin, Staff Services Analyst

DATE: June 18, 2013

SUBJECT: Approve Modification of Placer County Identity Theft Prevention Program as Required by the Fair and Accurate Credit Transactions Act of 2003 to remove references to the Redevelopment Successor Agency and the Redevelopment Agency

---

ACTION REQUESTED

Approve the modification of the Placer County Identity Theft Prevention Program as required by the Fair and Accurate Credit Transactions Act of 2003 to remove references to the Redevelopment Successor Agency and the Redevelopment Agency.

BACKGROUND

On May 12, 2009, your Board adopted a resolution approving the Placer County Identity Theft program. The purpose of the Identity Theft Prevention Program is to comply with the Federal Trade Commission regulations issued under the Fair and Accurate Credit Transactions Act of 2003 (FACTA). The Program assists staff in the detection, prevention and mitigation of identity theft by identifying and detecting identity theft "red flags," and by responding to such red flags in a manner that will prevent and mitigate identity theft.

Our Identity Theft Prevention Program requires the County Executive Office to annually review and update the Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the County and its covered accounts from identity theft.

In so doing, CEO surveyed all departments and determined that it is necessary to modify the Identity Theft Program to delete references to the Redevelopment Successor Agency and the Redevelopment Agency. The two programs under the Identity Theft Program that the former Redevelopment Successor Agency and the Redevelopment Agency managed that were considered to be at risk for identity theft are the Home Loan and Home Improvement Loan programs. These programs and associated accounts have been transferred to the Community Development Resource Agency (CDRA), which has been and continues to be an at-risk department for identity theft.

Other than deleting references to the Redevelopment Successor Agency and the Redevelopment Agency, no departments identified in the previous Program are recommended for deletion from the list of stakeholder departments. Stakeholder departments are:

- Administrative Services
- Child Support Services
- Community Development Resource Agency
- Facility Services
- Health and Human Services
- Treasurer-Tax Collector

CEO is required under the Program to bring any material changes to your Board for approval. The omission of the Redevelopment Successor Agency and the Redevelopment Agency are considered material changes.

FISCAL IMPACT

There is no fiscal impact to the modification of the Placer County Identity Theft Prevention Program by your Board nor to the implementation of the Program by stakeholder departments.

Attachment:

Placer County Identity Theft Prevention Program – June 18, 2013 update (deletions in strike-through text, additions in underlined text)

County of Placer
Identity Theft Prevention Program
June 18, 2013

Purpose

The purpose of the Identity Theft Prevention Program ("ITPP" or "Program") is to comply with the Federal Trade Commission regulations issued under the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The Program will assist staff in the detection, prevention and mitigation of identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent and mitigate identity theft.

Background

The Federal Trade Commission regulations governing the Identity Theft Prevention Program, adopted as 16 CFR § 681.2 (referred to as the "FTC Regulations"), require creditors to develop and provide a written program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Recently, FACTA has been amended to require that all creditors (including local government agencies that defer payments for goods or services) establish policies and procedures to help prevent identity theft. Under the FTC Regulations, "creditor" is a person that extends, renews or continues credit, and defines "credit," in part, as the right to purchase property or services and defer payment. The FTC Regulations include utility companies in the definition of creditor.

The FTC Regulations define "covered account," in part, as an account that a creditor provides for personal, family or household purposes that is designed to allow multiple payments or transactions or any other account that the creditor maintains for which there is a foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

The County has determined that it is a "creditor" under the FTC Regulations based on the activities of certain departments and consequently is required to have an Identity Theft Prevention Program in place. The departments, which are considered to be Stakeholder Departments, are:

- Administrative Services
- Child Support Services
- Community Development Resources Agency
- Facility Services
- Health & Human Services
- ~~Redevelopment Successor Agency (CDRA)~~
- Treasurer-Tax Collector

The FTC Regulations specify guidelines that should be considered in the development of the Program, taking into account the past incidents of identity theft with respect to the County's covered accounts and the County's assessment of the risk of future incidents. Accordingly, the County's Program provides a basic framework governing the County's policies and procedures for the identification, prevention and mitigation of incidents of identity theft with respect to the County's covered accounts. In developing the Program, the County has considered relevant "red flags" (see Definitions section, page 5) outlined in the FTC Regulations which are patterns, practices, or specific activities that indicate the possible existence of identity theft with respect to a covered account.

Consistent with the FTC Regulations, the initial Program was and policy was approved in May, 2009 by the Board of Supervisors. The implementation and administration of the Program is overseen by the County Executive Office.

The Federal Trade Commission also has issued regulations, adopted as 16 CFR § 681.1, to require users of consumer credit reports to develop policies and procedures relating to notices regarding address discrepancies from a consumer reporting agency. The County uses consumer credit reports for a variety of purposes such as: obtaining credit information regarding loan applicants, establishing deferred payment plans, and locating delinquent debtors. The departments that use the consumer credit reports for these purposes are listed above as Stakeholder Departments in the paragraph where the County determined that it acts as a "creditor." In addition, the County uses consumer credit information for conducting background checks in the County's hiring process for specific positions. This is done at the Office of the Sheriff. It was determined that FACTA does not apply in these cases because only part of the consumer information is used, the data is not retained at the County and notices of address discrepancy are not sent to the County.

Definitions

The following definitions apply to the Identity Theft Prevention Program (ITPP).

(a) "Covered account" means (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(b) "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 therefore.

(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 and includes utility companies and telecommunications companies.

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

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

(f) "Loan Programs" mean the County loan programs managed by ~~the~~ Placer County ~~Redevelopment Agency~~.

(g) "Personal 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:

i) Name, 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;
ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation.
iii) Unique electronic identification number address or routing code.
iv) Telecommunication identifying information or access device as defined in 18 U.S.C.1029(e),which states: any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument); means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

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

(i) "Service provider" means a person that provides a service directly to the County.

(j) "Stakeholder Department" means a County department that is impacted by FACTA. As of ~~May 2011~~ **June 2013**, the impacted departments and the reason that they are impacted are:

Administrative Services – Administers programs in Revenue Services division for creditors and thus is at risk for identity theft.

Child Support Services – accesses personal and financial information of customers from state sources and uses the data to enact wage garnishments and similar actions.

Community Development Resource Agency – CDRA accepts bonds and securities to guarantee completion of projects. Those funds are held, by project, in trust funds or for paper securities, bonds, letter of credits and assigned accounts, locked in a fire proof safe in the CDRC.

In addition, CDRA administers Home Loan and Home Improvement Loan programs, which require clients to enter into a repayment agreement with personal information.

Facility Services – Tipping fees for the West Placer Waste Management Authority and sewer fees are billed for certain individuals monthly. Credit information is maintained.

Health & Human Services – Provides payment plans for some patrons of the medical clinic.

Treasurer-Tax Collector – Uses client information to implement the mPOWER program.

Risk Assessment

(1) The County is a creditor due to its provision or maintenance of covered accounts for loan programs (including mPOWER), child support payments, general assistance, debt collection and medical services.

(2) The County has not encountered any reported incidents related to identity theft to date involving the County's covered accounts.

(3) The County limits access to personal identifying information to those employees responsible for or otherwise involved in opening, managing, or restoring covered accounts or accepting payment for use of covered accounts.

(4) The County must comply with many regulations that protect an individual's right to privacy such as HIPAA, AB2985 (2006) Foster Youth Identity Theft, SB1104 Welfare and Institutions code, and so forth.

(5) The County has well established Information Technology (IT) security policies that cover the computer systems that store the personal information.

(6) In addition to County security policies and procedures, each department has security policies and procedures of their own to ensure that account information is kept secure.

(7) The County has secure campuses where employees must pass through a security network to obtain physical access.

(8) Access to covered accounts is limited to authorized County personnel.

(9) Each Stakeholder department has established procedures for opening and maintaining covered accounts.

Outside Service Providers

As listed above, the County uses services providers to assist in collecting accounts. Each Stakeholder Department is responsible for the oversight of their service providers.

Categories and Types of Red Flags Applicable to Accounts[1]

Because of the wide range of County activities, each Stakeholder Department identifies the categories and types of red flags, as listed in Appendix A that are unique to their situation.

Prevention and Mitigation of Identity Theft

Existing Accounts

(1) In the event that any County 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 will use his/her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If such employee determines that identity theft or attempted identity theft is likely or probable, such employee will report such red flags to his/her immediate supervisor. If such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee will convey this information to his/her supervisor who may in his/her discretion determine that no further action is necessary. If it is determined that further action is necessary, a County employee will perform one or more of the following responses, as determined to be appropriate by his/her supervisor:

   a. Notify the customer regarding the information that indicates the threat of identity theft;
   b. Close the account.
   c. If applicable, cease attempts to collect additional charges from the customer and decline to sell or transfer 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. If applicable, notify a debt collector of the discovery of likely or probable identity theft relating to a customer account that has been sold to or is being serviced by such debt collector in the event that a customer's account has been transferred to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;
   e. In the event that someone other than the customer has accessed the customer's covered account causing additional charges to accrue or accessing personal identifying information, notify the Department Director or the Director's designee. The Department Director or the Director's designee will then determine whether further notifications to the County Executive Office, County Counsel and/ or the Placer County Sheriff are warranted under the circumstances; or
   f. Take other appropriate action to prevent or mitigate identity theft.

New Accounts

(2) In the event that any County employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect to an application for a new account, such employee will use his/her

[1] A full list of Red Flags listed in the Federal Trade Commission Regulations for creditors to consider in adopting their identity theft prevention programs can be found at Appendix A.

discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If such employee determines that identity theft or attempted identity theft is likely or probable, such employee will report such red flags to his/her immediate supervisor. If such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee will convey this information and determine that no further action is necessary. If further action is necessary, a County employee will perform one or more of the following responses, as determined to be appropriate by his/her manager:

a. Request additional identifying information from the applicant;
b. Deny the application for the new account;
c. Notify the Stakeholder Department Director or the Director's designee, who will then determine whether further notifications to the County Executive Office, County Counsel and/or the Placer County Sheriff are warranted under the circumstances; or
d. Take other appropriate action to prevent or mitigate identity theft.

Updating the Program (Program Administration)

The County Executive Office ("CEO") will annually review and 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 County and its covered accounts from identity theft. In so doing, the CEO will consider the following factors and exercise its discretion in amending the program:

(1) The County's experiences with identity theft;
(2) Updates in methods of identity theft;
(3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
(4) Updates in the types of accounts that the County offers or maintains; and
(5) Updates in service provider arrangements.

Program Administration

Senior Staff within the Stakeholder Departments ("Senior Staff") are responsible for oversight of the Program and for Program implementation and will be responsible for preparing reports to the County Executive Office related to compliance with the Program and recommendations for changes to the Program ("Program Reports"). The County Executive Office will review Program Reports and will oversee the implementation of material changes to the Program, as necessary in the opinion of the County Executive, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program, as determined by the County Executive, will be submitted to the Board of Supervisors for acceptance.

(1) Senior Staff will report to the County Executive 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:

a. The effectiveness of the policies and procedures of County in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
b. Service provider arrangements;
c. Significant incidents involving identity theft and management's response; and
d. Recommendations for material changes to the Program.

(2) Senior Staff within each Stakeholder Department are responsible for providing training to all employees within the Stakeholder Department who are 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 will exercise his or her discretion in determining the amount and substance of training necessary.

Appendix A

Categories and Types of Red Flags

The red flags listed below are set forth in the FTC (Federal Trade Commission) Regulations for creditors to consider in adopting their identity theft prevention programs. The types of red flags listed below do not apply to all covered accounts.

(1) Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:

a. A fraud or active duty alert that is included with a consumer report;
b. A notice of credit freeze in response to a request for a consumer report;
c. A notice of address discrepancy provided by a consumer reporting agency;
d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    i. A recent and significant increase in the volume of inquiries;
    ii. An unusual number of recently established credit relationships;
    iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
    iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(2) Suspicious documents. Examples of suspicious documents include:

a. Documents provided for identification that appear 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 that is inconsistent with external information sources used by the financial institution or creditor. For example:
    i. The address does not match any address in the consumer report; or
    ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth;

c. 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 financial institution or creditor;
d. 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;
e. The SSN provided is the same as that submitted by other applicants or customers for the same type of covered account;
f. 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 for the same type of covered account;
g. 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;
h. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor; or
i. 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, the County 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;
    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 County is notified that the customer is not receiving paper account statements.
g. The County is notified of unauthorized charges or transactions in connection with a customer's account.
h. The County 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.