THE BOARD OF SUPERVISORS OF THE COUNTY OF STANISLAUS
ACTION AGENDA SUMMARY

DEPT: Chief Executive Office **BOARD AGENDA #** *B-3

Urgent ☐ **Routine** ☒ **AGENDA DATE** April 6, 2010

CEO Concurs with Recommendation YES ☒ **NO** ☐ **4/5 Vote Required YES** ☐ **NO** ■
(Information Attached)

SUBJECT:

Approval to Adopt the Proposed Identity Theft Prevention Program (ITPP) as the County's Red Flag Policy to Comply with the Amended Federal Fair and Accurate Credit Transaction Act of 2003

STAFF RECOMMENDATIONS:

Approve the adoption of the Identity Theft Prevention Program (ITPP) as the County's Red Flag policy to comply with the amended Federal Fair and Accurate Credit Transaction Act of 2003.

FISCAL IMPACT:

Implementation of the Identify Theft Prevention Program will assure the protection of individuals identifying information and protect the County from any financial liability associated with the theft of personal identifying information.

BOARD ACTION AS FOLLOWS:

No. 2010-183

On motion of Supervisor O'Brien , **Seconded by Supervisor** DeMartini
and approved by the following vote,
Ayes: Supervisors: O'Brien, Chiesa, Monteith, DeMartini, and Chairman Grover
Noes: Supervisors: None
Excused or Absent: Supervisors: None
Abstaining: Supervisor: None

1) X **Approved as recommended**
2) _____ **Denied**
3) _____ **Approved as amended**
4) _____ **Other:**
MOTION:

Christine Ferraro

ATTEST: **CHRISTINE FERRARO TALLMAN, Clerk** **File No.**

DISCUSSION:

The Identity Theft Prevention Program Policy (ITPP) is being established to comply with the Federal Trade Commission (FTC) regulations issued under the Fair and Accurate Credit Transactions (FACT) Act of 2003. The FTC regulations governing the Identity Theft Prevention Program, adopted as 16 CFR §681.2, 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. A covered account involves multiple payments or transactions where personal identifying information is maintained. In 2008, the FACT Act was 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. The regulations require that the Board approve the initial program.

The attached Identity Theft Prevention Program Policy for Stanislaus County has been written in response to the FTC's regulatory requirements. As part of the development of the policy a thorough analysis of the operations of all County departments was conducted to determine which activities might be subject to the Red Flag Rules, and to ensure that the County fully complies with the Red Flag Rules. The policy lists the impacted departments, categories and types of red flags. The impacted departments are responsible for implementing policies and procedures for situations unique to their departments. Departments are also able to adopt an Identity Theft Prevention Program specific to their department under this policy. Currently the Health Services Agency has adopted a policy specific to their organizational needs.

The Chief Information Officer and Chief Executive Office staff responsible for the development, implementation, and administration of this ITPP shall report to County's Board of Supervisors on an annual basis. The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the ITPP. The ITPP will also become part of the County's annual Internal Information Technology Security Assessment

This policy was developed with the assistance of legal counsel and has been reviewed by County Counsel.

POLICY ISSUES:

Approval of an Identity Theft Prevention Program will address the Board of Supervisors' priority of *Efficient delivery of public services* by ensuring the County will be in compliance with the Federal Fair and Accurate Credit Transaction Act of 2003.

STAFFING IMPACT:

There are no staffing impacts associated with this item. Existing staff will administer the ITPP policy.

CONTACT PERSON:

Nancy Bronstein, Deputy Executive Officer. (209)525-7685

I. The Purpose of the Identity Theft Prevention Program

The purpose of Stanislaus County's Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to persons from identity theft. Identity theft results in billions of dollars in losses each year to individuals and businesses.

Stanislaus County is also required to provide for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft because the County is a "creditor" with "covered accounts."

II. Definitions

A. Identity Theft – Identity theft is a fraud attempted or committed using identifying information of another person without authority.

B. Creditor – A creditor includes government entities who defer payment for goods or services (for example, payment for utilities, or payment plans for parking tickets).

C. Deferring Payments – Deferring payments refers to postponing payments to a future date and/or installment payments on fines or costs.

D. Covered Account – A covered account includes one that involves multiple payments or transactions. County departments with covered accounts are listed below. Any additional County departments with new covered accounts will comply with the policy at the time the account is created.

1. Behavioral Health and Recovery Services – Support care client repayment and patient fees for mental health services;

2. Community Services Agency - Provides general and other financial assistance and collects overpayments;

3. Health Services Agency – Provides medical services for which payment is made after the service has been provided;

4. Probation Department – Provides payment plan for institutional charges and court referred program costs;

5. Sheriff's Department – Collects ongoing payments for individuals on Alternative Work Programs; and

6. Treasurer Tax Collector – Provide collection services for money owed to the County.

E. Person - Person means any individual who is receiving goods and/or services from the County and is making payments on a deferred basis for said goods and/or services.

F. Red Flag – Detection or discovery of a Red Flag implicates the need to take action under

this ITPP to help prevent, detect, and correct identity theft.

III. Detecting "Red Flags" For Potential Identity Theft

A. Risk Factors for Identifying "Red Flags"

County will consider the following factors in identifying relevant "Red Flags":

1. The types of covered accounts the County offers or maintains;
2. The methods the County provides to open the County's covered accounts;
3. The methods the County provides to access the County's covered accounts; and
4. The County's previous experience(s) with identity theft.

B. Sources of "Red Flags"

The County will continue to incorporate relevant "Red Flags" into this ITPP from the following sources:

1. Incidents of identity theft that the County experiences;
2. Methods of identity theft that the County identifies that reflects changes in identity theft risks; and
3. Guidance from the County's Board of Supervisors who identify changes in identity theft risks.

C. Categories of "Red Flags"

The following Red Flags have been identified for the County's covered accounts:

1. Alerts, Notifications, or Warnings from a Consumer Reporting Agency:
    a. A fraud or active duty alert is included with a consumer report the County receives.
    b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
    c. A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a consumer substantially differs from the one the credit reporting agency has on file. See Section (V) (9) for specific steps that must be taken to address this situation.

d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or consumer, such as:

1) A recent and significant increase in the volume of inquiries;

2) An unusual number of recently established credit relationships;

3) A material change in the use of credit, especially with respect to recently established credit relationships; or

4) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution.

2. *Suspicious Documents:*

a. Documents provided for identification appear to have been forged or altered.

b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

d. Other information on the identification is not consistent with readily accessible information that is on file with the County, such as a signature card or a recent check.

e. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

3. *Suspicious Personally Identifying Information:*

a. Personal identifying information provided is inconsistent when compared against external information sources used by the County. For example:

1) The address does not match any address in the consumer report; or

2) 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 a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.

c. Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the County. For example:

1) The address on an application is the same as the address provided on fraudulent application;
2) The phone number on an application is the same as the phone number provided on a fraudulent application;

d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the County. For example:

1) The address on an application is fictitious, a mail drop, or a prison; or

2) The phone number is invalid, or is associated with a pager or answering service.

e. The SSN provided is the same as that submitted by other persons currently being served by the County.

f. The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the County.

g. The person opening the covered account or the 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 provided is not consistent with personal identifying information that is on file with the County.

i. The person opening the covered account 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:*

a. A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.

b. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is:

1) Nonpayment when there is no history of late or missed payments; or

2) A material change in electronic fund transfer patterns in connection with a payment.

c. A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.

d. Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account.

e. The County is notified that the person is not receiving paper account statements.

f. The County is notified of unauthorized transactions in connection with a person's covered account.

5. *Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:*

The County is notified by a person with a covered account, a victim of identity theft, a law enforcement authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.

IV. Measures to Detect "Red Flags"

The County shall do the following to aid in the detection of "Red Flags:"

A. When a new covered account is open, the County shall obtain identifying information about, and information verifying the identity of, the person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).

The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or invoice/statement for property taxes.

B. Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the County.

The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.

V. Preventing and Mitigating Identity Theft

One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:

1. Monitor the covered account for evidence of identity theft;

2. Contact the person who holds the covered account;

3. Change any passwords, security codes, or other security devices that permit access to a covered account;

4. Reopen the covered account with a new account number;

5. Not open a new covered account for the person;

6. Close an existing covered account;

7. Not attempt to collect on a covered account or not sell a covered account to a debt collector;

8. Notifying law enforcement;

9. Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the County shall take the necessary steps to form a reasonable belief that the County knows the identity of the person for whom the County obtained a credit report, and reconcile the address of the consumer with the credit reporting agency, if the County establishes a continuing relationship with the consumer , and regularly, and in the course of business, provides information to the credit reporting agency; or

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

VI. Updating the ITPP

The County shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, and/or to reflect changes in risks to the safety and soundness of the County from identity theft, based on the following factors:

1. The experiences of the County with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent and mitigate identity theft;

4. Changes in the types of covered accounts that the County maintains; and

5. Changes in the business arrangements of the County, including service provider arrangements.

VII. Methods for Administering the ITPP

A. Oversight of the ITPP

Oversight is by the Chief Executive Office, Chief Information Officer. Responsibilities shall include:

1. Assigning specific responsibility for the ITPP's implementation;

2. Reviewing reports prepared by the staff regarding compliance of the ITPP; and

3. Approving material changes to the ITPP as necessary to address changing identity theft risks.

B. Reports

1. *In General.* The Chief Information Officer and Chief Executive Office staff responsible for the development, implementation, and administration of this ITPP shall report to the County's Board of Supervisors on an annual basis.

2. *Contents of Report.* The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the ITPP.

3. *Oversight of Service Provider Arrangements.* Whenever the County engages a service provider to perform an activity in connection with one or more covered accounts the County shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the County shall require our service contractors, by contract, to have policies and procedures to detect relevant "Red Flags" that may arise in the performance of the service provider's activities, and either report the "Red Flags" to the County, or to take appropriate steps to prevent or mitigate identity theft.