California State University Stanislaus
Identity Theft Prevention
("Red Flags")
Implementation Plan

VERSION CONTROL

Document Title:	California State University Stanislaus Identity Theft Prevention Implementation Plan

Review/Approval History

Date	By	Action	Pages
9/22/2009	C. Washington	Submitted to Board of Trustees	All
11/1/2009	C. Whitman	Adapted for Use at CSU Stanislaus	All

Acknowledgements:

CSU Stanislaus greatly appreciates the support of the following individuals who assisted in the development of this implementation plan:

- Laura Carrizales, CSU San Bernardino
- Andrew Jones, CSU Chancellor's Office
- Sheryl Okuno, CSU Los Angeles
- Maryann S. Rozanski, CSU Long Beach
- Cheryl Washington, CSU Chancellor's Office

TABLE OF CONTENTS

1.0 INTRODUCTION

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which required “creditors” to adopt policies and procedures to prevent identity theft. These requirements are described in section 114 of FACTA and are known as the “Red Flags Rule.” In November 2007, final rules implementing section 114 of FACTA were issued by the Federal Trade Commission, but because certain aspects of the rules needed clarification, the FTC delayed enforcement of the new rules until November 1, 2009.

The Red Flags Rule applies to financial institutions and “creditors” that offer or maintain accounts that provide for multiple transactions primarily for personal, family, or household purposes. The definition of “creditor” is broad, and includes any entity that regularly extends credit. Institutions are considered creditors if they provide goods or services that are not fully paid for in advance or allow individuals to defer payment for goods or services. The rule does not apply if the institution is merely accepting a credit card for payment.

There are many instances where CSU campuses meet the definition of a “creditor” under the Red Flags Rule. Executive Order 632 provides express permission for campuses to institute installment payment plans for the state university fee and nonresident tuition. Many, if not all, campus housing programs also accept installment payments. There also are a number of activities in the financial aid area, such as Perkins Loan transactions, that bring campuses within the Act’s definition of a creditor.

An institution that meets the definition of a “creditor” must then determine if any of the accounts it handles are “covered accounts” as defined by the Act. Under the Act, a covered account is one used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card accounts; mortgage loans; automobile loans; margin accounts; cell phone accounts; utility accounts; checking accounts; and savings accounts. A covered account is also any account for which there is a foreseeable risk of identity theft. The Red Flags Rule and the FTC’s guidance on it indicate that covered accounts include certain types of arrangements in which an individual establishes a "continuing relationship" with the enterprise, including billing for previous services rendered. Although the definition of a covered account is neither very clear nor specific, it appears that any type of account or payment plan that involves multiple transactions or multiple payments in arrears is likely a "covered account." Thus, it seems that EO 632 installment payment plan accounts, housing program installment payment accounts, and various accounts in the financial aid area are among the type of accounts that qualify as covered accounts.

Red Flags are defined as those events which should alert an organization to potential risk of identity theft. Under the Red Flags Rule, the CSU is required to establish a documented Identity Theft Prevention program that provides for the identification, detection, and response to patterns, practices, or specific activities that could indicate identity theft.

2.0 PURPOSE

The CSU Identity Theft Prevention Implementation Plan is designed to help campuses develop an identity theft prevention program that complies with the Red Flags Rule. In designing its program, a campus may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the institution from identity theft.

3.0 DEFINITIONS

Account means a continuing relationship established by a person with a campus to obtain a product or service for personal, family, household or business purposes. Account includes:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and
- A deposit account

A **campus** includes any campus or satellite campus of the California State University and the Chancellor's Office of the California State University.

A **creditor** is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college or university is a "creditor" are:

- Participation in the Federal Perkins Loan program;
- Participation as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students, faculty or staff; or
- Offering a plan for payment of tuition or fees throughout the academic term, rather than requiring full payment at the beginning of the term.

A **covered account** is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

Identity Theft is the act of fraud committed using the personal identifying information of another person.

A **red flag** is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Service provider means a person that provides a service directly to the campus.

4.0 THE PROGRAM

4.1. Program Requirements

Each campus that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program ("**Program"**) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or the management of any existing covered account.

The **Program** must include reasonable policies and procedures to:

- Identify covered accounts;

- Identify relevant Red Flags for each type of covered accounts;
- Detect Red Flags;
- Respond to Red Flags; and,
- Ensure the campus program is updated periodically to identify additional Red Flags and to reflect changes in risk to individuals from identity theft.

In designing its program, a campus may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the institution from identity theft.

4.2. Identify Covered Accounts

Each campus must periodically determine whether it offers or maintains covered accounts. Covered accounts may include:

- Student loans.
- Installment payments and short term loans.
- Accounts that are created for ongoing services and allow students to reimburse the University when billed over a period of time.
- Any type of collection account.

Examples of potential covered accounts are provided in Appendix A.

4.3. Identify Relevant Red Flags

As stated in the definition, a "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft. In order to identify relevant red flags, University departments that offer and manage covered accounts must review and evaluate the methods used to open covered accounts, to allow access to covered accounts, and any previous known occurrences of identity theft.

4.3.1. Categories of Red Flags

The **Program** should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are provided below.

4.3.1.1. Alerts, Notifications or Warnings from Consumer Reporting Agency

Examples of Red Flags include:

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- 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:
    - A recent and significant increase in the volume of inquires;
    - An unusual number of recently established credit relationships;

    - A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a campus.

4.3.1.2. Suspicious Documents

Examples of Red Flags include:

- Documents provided 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 applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the campus, 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.

4.3.1.3. Suspicious Personal Identifying Information

Examples of Red Flags include:

- Personal identifying information provided is inconsistent when compared against external information sources used by the campus. For example:
    - The address does not match any address in the consumer report; or
    - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the campus. For example:
    - The address on an application is the same as the address provided on a fraudulent application; or
    - The phone number on an application is the same as the number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the campus. For example:
    - The address on an application is fictitious, a mail drop, or a prison; or
    - The phone number is invalid, or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the address number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

- 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.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the campus.
- For campuses that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4.3.1.4. Unusual Use of, or Suspicious Activity Related to, the Covered Account

Examples of Red Flags include:

- Shortly following the notice of a change of address for a covered account, the campus receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
    - The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
    - The customer fails to make the first payment or makes an initial payment but no subsequent payments.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    - Nonpayment when there is no history of late or missed payments;
    - A material increase in the use of available credit;
    - A material change in purchasing or spending patterns;
    - A material change in electronic fund transfer patterns in connection with a deposit account; or
    - A material change in telephone call patterns in connection with a cellular phone account.
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The campus is notified that the customer is not receiving paper account statements.
- The campus is notified of unauthorized charges or transactions in connection with a customer's covered account.

4.3.1.5. Notice from Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Campus

Examples of Red Flags include:

- The campus is notified by a customer, 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.

4.4. Detect Red Flags

The **Program's** policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account;
- Authenticating individuals;
- Monitoring transactions; and
- Verifying the validity of change of address requests, in the case of existing covered accounts.

4.5. Respond to Red Flags

The **Program's** policies and procedures should provide for appropriate responses to Red Flags the campus has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a campus should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to an individual's account records held by the campus or third party, or notice that a individual has provided information related to a covered account held by the campus to someone fraudulently claiming to represent the campus or to a fraudulent website.

Appropriate responses may include the following:

- Monitoring a covered account for evidence of identity theft;
- Contacting the individual;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

5.0 PROGRAM ADMINISTRATION

Each campus must provide for the continued administration of the **Program.** The campus President (or his/her designee) must approve the initial campus program and assign program oversight responsibilities to a campus program administrator. The program administrator must be a campus senior manager (e.g., CIO, VP of Administration or Enrollment Management, etc,).

Program administration responsibilities include:

- Developing and implementing the campus program;

- Reviewing reports prepared by staff regarding compliance with the campus **Program**;
- Approving material changes to the **Program** as necessary to address changing identity theft risks;
- Training staff, as necessary, to implement the **Program** effectively; and
- Exercising appropriate and effective oversight of service provider arrangements.

5.1. Reporting Requirements

Staff responsible for implementing the **Program** must submit a compliance report to the program administrator ***at least annually.*** The report should address material matters related to the **Program** and evaluate issues such as:

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of 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 **Program**.

5.2. Program Review

The program administrator should review the **Program** (including the Red Flags determined to be relevant) annually to reflect changes in risks to individuals from identity theft, based on factors such as:

- The experience of the campus with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the types of accounts that the campus offers or maintains; and,
- Changes in service provider agreements.

The System-wide Office of Information Security Management will periodically validate with the campus program administrator the progress and efforts made related to compliance with this implementation plan.

5.3. Staff Training

The program administrator should work with campus departments to ensure staffs are trained as necessary to carry out the requirements of the program effectively.

5.4. Oversight of Service Provider Arrangements

The University remains responsible for compliance with the Red Flags Rule even if it outsources operations to a third party service provider. Whenever a campus engages a service provider to perform an activity in connection with one or more covered accounts, the campus should 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. For example, a campus could require the service provider 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 campus, or to take appropriate steps to prevent or mitigate identity theft.

The Red Flags Rule also applies to "financial institutions," generally defined as banks, thrifts, credit unions, and other institutions that offer transaction accounts[1]. Colleges and universities that offer students the option of having their student ID also operate as a Visa or MasterCard debit card should coordinate with the bank through which such services are offered to ensure that the bank has an adequate identity theft prevention program in place.

[1] A transaction account is a deposit or other account from which the account holder may make payments or transfers. Transaction accounts including checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts. See 12 U.S.C. §461(b)(1)(C).

APPENDIX A: Potential Covered Accounts

I. General Financial Services

a. Campus Tuition and Fee Deferred Payment Plans
b. Campus Billing and Accounts Receivable
c. Visiting Scholar Payments
d. International Student Plans
e. Internal Student Plans
f. Payroll
g. University Corporate Credit Card
h. Campus Student ID Debit Card

II. Financial Aid

a. Scholarships
b. Tuition Remission
c. Fellowships

III. Student and Parent Loans

a. Stafford Loans
b. Perkins Loans
c. Plus Loans
d. Institutional Loans
e. Campus Emergency Loans for Students
f. Parent Loans
g. Faculty Loans
h. Employee and Staff Loans
i. Mortgage Origination Program (MOP) Loans

IV. Housing

a. Student and/or Student Family
b. Faculty Rental and For Sale

V. Health Services

a. Student Health Insurance Plans
b. Faculty Health Insurance Plans
c. Employee and Staff Insurance Plans
d. Student Health Centers

VI. Miscellaneous

a. Dining Services
b. Athletic Services
c. Counseling Services
d. Continuing Education
e. Human Resources

APPENDIX B: Reporting Procedure

California State University | Stanislaus

Subject:	**Identity Theft Red Flag and Security Incident Reporting Procedure**		
Department:	**Office of Information Technology**	Issue Date:	**November 2009**
References:	• **Fair and Accurate Credit Transactions Act of 2003 (FACTA)** • **California Information Practices Act (IPA) of 1977**	Revision Date:	
Web Links:	• **http://www.csustan.edu/oit/PoliciesPlans.html**	Expiration Date:	**N/A**

I. PURPOSE

The purpose of the *Identify Theft Red Flag and Security Incident Reporting Procedure* is to provide information to assist individuals in 1) detecting, preventing, and mitigating identity theft in connection with the opening of a "covered account" or any existing "covered account" or who believe that a security incident has occurred and 2) reporting a security incident.

II. BACKGROUND

Security Incident

Existing California law requires that any organization that owns computerized data that includes personal information shall disclosure any breach of security of the system following discovery or notification of the breach in the security of the system to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Red Flag Rules

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring "creditors" to adopt policies and procedures to prevent identify theft.

In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires "financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags."

III. DEFINITIONS

Covered Account – A covered account is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

Creditor – A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college or university is a "creditor" are:

- Participation in the Federal Perkins Loan program;
- Participation as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students, faculty or staff;
- Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

Personal Information – Specific items of personal information identified in CA Civil Code Sections 1798.29 and 1798.3. This information includes an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security Number, driver's license/California identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Red Flag – A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Security Incident – A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

IV. IDENTIFICATION OF RED FLAGS

Broad categories of "Red Flags" include the following:

- **Alerts** – alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.

- **Suspicious Documents –** such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.

- **Suspicious Personal Identifying Information** – such as discrepancies in address, Social Security Number, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.

- **Unusual Use or Suspicious Account Activity** –such as material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges;

- **Notice from Others Indicating Possible Identify Theft** –such as the institution receiving notice from a victim of identity theft, law enforcement, or another account holder reports that a fraudulent account was opened.

V. DETECTION OF RED FLAGS

Detection of Red Flags in connection with the opening of covered accounts as well as existing covered accounts can be made through such methods as:

- Obtaining and verifying identity;
- Authenticating customers;
- Monitoring transactions

A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the University or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags.

VI. RESPONSE TO RED FLAGS

The detection of a Red Flag by an employee shall be reported to the Information Security Officer and their appropriate administrator. Based on the type of red flag, the appropriate administrator and the Information Security Officer together with the employee will determine the appropriate response.

VII. SECURITY INCIDENT REPORTING

An employee who believes that a security incident has occurred, shall immediately notify their appropriate administrator and the Information Security Officer. After normal business hours, notification shall be made to the University police (209) 667-3114.

VIII. SERVICE PROVIDERS

The University remains responsible for compliance with the Red Flag Rules even if it outsources operations to a third party service provider. The written agreement between the University and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate whether the service provider is responsible for notifying only the University of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigated identify theft.

IX. TRAINING

All employees who process any information related to a covered account shall receive training following appointment on the procedures outlined in this document. Refresher training may be provided annually.

CONTACT INFORMATION

Information Security Officer
Office of Information Technology
California State University, Stanislaus
One University Circle
Turlock, CA 95382
209-667-3343
iso@csustan.edu