## REVIEW/APPROVAL HISTORY

**Document Title:** Identity Theft Prevention “Red Flags” Program  
**Author:** Brooke F. Banks, Information Security Officer

<table>
<thead>
<tr>
<th>Date</th>
<th>By</th>
<th>Action</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/30/2009</td>
<td>Bill Post, Vice Provost for Information Resources and CIO</td>
<td>Review and Approval</td>
<td>All</td>
</tr>
<tr>
<td>11/04/2009</td>
<td>Drew Calandrella, Vice President for Student Affairs</td>
<td>Review and Approval</td>
<td>All</td>
</tr>
<tr>
<td>08/20/2010</td>
<td>Lori Hoffman, Vice President for Business and Finance</td>
<td>Review and Approval</td>
<td>All</td>
</tr>
<tr>
<td>11/16/2010</td>
<td>Paul Zingg, President</td>
<td>Review and Final Approval</td>
<td>All</td>
</tr>
</tbody>
</table>
# Table of Contents

Introduction ................................................................................................................................... 4  
Purpose.......................................................................................................................................... 5  
Definitions...................................................................................................................................... 5  
Identification of Covered Accounts ............................................................................................. 6  
Identification of Red Flags............................................................................................................ 6  
Detection of Red Flags.................................................................................................................. 6  
Response to Red Flags.................................................................................................................... 7  
Training.......................................................................................................................................... 7  
Service Providers .......................................................................................................................... 7  
Program Administration ............................................................................................................... 8  

Appendix A – Covered Accounts ................................................................................................. 9  
Appendix B – Examples of Red Flags.......................................................................................... 10  
Appendix C – Identity Theft “Red Flags” Compliance Report ....................................................... 13  
Appendix D - References ............................................................................................................ 14
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”.

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. Additionally, there 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 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. 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.

Red Flags are defined as those events which should alert an organization to potential risk of identity theft. Under the Red Flags Rule all CSU campuses are 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.
Purpose

The purpose of the Identity Theft Prevention “Red Flags” Program (“Program”) is to provide information to assist individuals in detecting, preventing, and mitigating identity theft in connection with the opening of a covered account or the management of any existing covered account.

The Program includes procedures to:

• Identify covered accounts
• Identify relevant Red Flags for each type of covered account
• Detect Red Flags
• Respond to Red Flags
• Ensure the Program is updated periodically to identify additional Red Flags and to reflect changes in risk to individuals from identity theft.

Definitions

Account – A continuing relationship established by a person with a campus to obtain a product or service for personal, family, household or business purposes. Accounts include an extension of credit, such as the purchase of property or services involving deferred payment and a deposit account.

Covered Account – A consumer account designed to permit multiple payments and 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 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

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

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

Service Provider – A person that provides a service directly to the campus.
Identification of Covered Accounts

Covered accounts are those accounts where a formal financial relationship exists, such as extending credit. Covered accounts do include transactions for goods or services where a formal financial relationship is not established.

University departments that offer and manage accounts designed to permit multiple payments and transactions, where payments are deferred, are responsible for notifying the Program Administrator of the existence of a covered account. A current list of covered accounts can be found in Appendix A.

Identification of Red Flags

University departments that offer and manage covered accounts (account owners) are responsible for identifying red flags related to their covered accounts. In order to identify relevant red flags, departments 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.

Broad categories of “Red Flags” include but are not limited to the following:

- **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 to, the Covered Account** – 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 in Connection with Covered Accounts Held by the Campus** – 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.

Examples of “Red Flags” for each category can be found in Appendix B.

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.
Response to Red Flags

The detection of a Red Flag by an employee shall be reported to the Information Security Officer and appropriate department 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.

Training

University departments that offer and manage covered accounts (account owners) are responsible for providing training on the procedures outlined in this document and any department procedures related to the Program following appointment.

The program administrator shall provide general Red Flags training on an as needed basis. Refresher training may be provided annually.

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 mitigate identify theft.
Program Administration

The campus Information Security Officer will serve as program administrator for the Program. Program administration responsibilities include:

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

Reporting Requirements

Staff responsible for implementing the Program must submit a compliance report to the program administrator at least annually; see the template in Appendix C. 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
- Recommendations for material changes to the Program

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
- Changes in service provider agreements

The System-wide Office of Information Security Management will periodically validate with the program administrator the progress and efforts made related to compliance with this implementation plan.
## Appendix A – Covered Accounts

<table>
<thead>
<tr>
<th>Covered Account</th>
<th>Account Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Financial Services</strong></td>
<td></td>
</tr>
<tr>
<td>Campus Tuition &amp; Fee Deferred Payment Plans</td>
<td>Director, Student Financial Services</td>
</tr>
<tr>
<td>Campus Billing and Accounts Receivable</td>
<td></td>
</tr>
<tr>
<td>Student</td>
<td>Director, Student Financial Services</td>
</tr>
<tr>
<td>Non-Student</td>
<td>Director, Accounting Operations</td>
</tr>
<tr>
<td>Payroll</td>
<td>Chief Human Resources Officer</td>
</tr>
<tr>
<td>University Corporate Credit Card</td>
<td>Director, Accounting Operations</td>
</tr>
<tr>
<td><strong>Student and Parent Loans</strong></td>
<td></td>
</tr>
<tr>
<td>Perkins Loans</td>
<td>Director, Financial Aid</td>
</tr>
<tr>
<td><strong>Housing</strong></td>
<td></td>
</tr>
<tr>
<td>Student Housing</td>
<td>Director, Univ Housing &amp; Food Service</td>
</tr>
<tr>
<td><strong>Health Services</strong></td>
<td></td>
</tr>
<tr>
<td>Student Health Center</td>
<td>Director, Student Health Service</td>
</tr>
<tr>
<td>Family PACT Program</td>
<td>Director, Student Health Service</td>
</tr>
<tr>
<td>Gardasil by Blue Ox Program</td>
<td>Director, Student Health Service</td>
</tr>
<tr>
<td><strong>Miscellaneous</strong></td>
<td></td>
</tr>
<tr>
<td>Communications Account Services</td>
<td>Director, Communications Services</td>
</tr>
<tr>
<td>Continuing Education</td>
<td>Associate Dean, Regional &amp; Cont. Ed</td>
</tr>
</tbody>
</table>
Appendix B – Examples of Red Flags

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 inquiries;
  - 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.

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.

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
o 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:
  o The address on an application is fictitious, a mail drop, or a prison; or
  o 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.

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:
  o 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
  o 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:
  o Nonpayment when there is no history of late or missed payments;
  o A material increase in the use of available credit;
  o A material change in purchasing or spending patterns;
  o A material change in electronic fund transfer patterns in connection with a deposit account;
  or
  o 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.
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.
Appendix C – Identity Theft “Red Flags” Compliance Report Template

Department ________________________________

Date ____________________

Covered Accounts & Red Flags
List all covered accounts in your department and indicate where documentation exists of red flags.

Red Flag Events
List any significant incidents involving identity theft and management’s response.

Training
List all employees who have received Identity Theft Prevention “Red Flags” training and the date training was provided.

Service Provider Agreements
For any third party service provider agreements, provide validation that these parties have reasonable policies and procedures to detect relevant Red Flags that may arise in the performance of their agreements.

Recommendations
Do you recommend any material changes to the Identity Theft Prevention “Red Flags” Program?
Appendix D - References

The CSU, Chico Identity Theft “Prevention” Red Flag Program complies with federal and state regulations and California State University policy specified in documents at the following links: