



# CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: <b>Identity Theft Prevention Program</b>	
Department: <b>Information Security Management and Compliance</b>	Reference No.:
Division: <b>Administration and Finance</b>	Issue Date: <b>January 2009</b>
References: <b>Fair and Accurate Credit Transactions Act of 2003 (FACTA) California Information Practices Act (IPA) of 1977 CSU Identity Theft Protection Implementation Plan</b>	Revision Date: <b>October 2009</b>
Web Links: <b><a href="http://daf.csulb.edu/offices/vp/information_security">http://daf.csulb.edu/offices/vp/information_security</a></b>	Expiration Date: <b>N/A</b>

## I. PURPOSE

The purpose of the *Identify Theft Prevention Program* is to detect, prevent, and mitigate identity theft in connection with the opening of a “covered account” or the management of any existing covered account.

## II. BACKGROUND

### Red Flag Rules

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACTA) which required “creditors” to adopt policies and procedures to prevent identify theft. These requirements are described in Section 114 of FACTA and are known as the “Red Flags Rule”.

The Red Flags 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

**Account** – A continuing relationship established by a person with the University to obtain a product or service for personal, family, household or business purpose. Accounts include:

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

**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.

**Red Flag** – A red flag is 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 University.

#### IV. COVERED ACCOUNTS

CSULB Covered Accounts include, but may not be limited to:

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

#### V. IDENTIFICATION OF RED FLAGS

Broad categories of “Red Flags” include the following:

- **Alerts, Notification or Warnings from Consumer Reporting Agencies**

*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.

- **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
  - 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.
- **Unusual Use or Suspicious Account Activity**  
*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.
  - **Notice from Others Indicating Possible Identify Theft**  
*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.

## **VI. 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
- Verifying the validity of change of address requests in the case of existing covered accounts.

## **VII. RESPONSE TO RED FLAGS**

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

Appropriate responses may include:

- 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.

## **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 mitigate identity theft.

## **IX. TRAINING**

All employees who process any information related to a covered account shall receive training to understand their responsibilities associated with the *Identity Theft Prevention Program*.

## **X. ANNUAL PROGRAM REVIEW AND REPORTING REQUIREMENTS**

The Director, Information Security Management and Compliance shall review these requirements annually to evaluate and modify them as appropriate:

- 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.

Factors which may result in changes to these procedures include;

- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the types of accounts offered or maintained by the University;
- Changes in Service Provider agreements.

## **FURTHER INFORMATION**

Information Security Management, Audit and Compliance  
iso@csulb.edu.  
(562) 985-4862