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 Flag Rule applies to financial institutions and "creditors" that offer or maintain accounts that

3.0

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.

o

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.

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.**

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:

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

APPENDIX B: Reporting Procedure

Subject:		**Identity Theft Red Flag and Security Incident Reporting Procedure**	
Department:	**Office of Information Technology**	Issue Date:	**November 2009**
References:		Revision Date:	
	Fair and Accurate Credit Transactions Act of 2003 (FACTA)		

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.

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.