STOCKTON UNIVERSITY

PROCEDURE

Identity Theft Prevention Program

Procedure Administrator: Director of Risk Management and Environmental/Health/Safety
Authority: Fair and Accurate Credit Transactions Act of 2003, 16 CFR 681.2
Effective Date: May 6, 2009; February 16, 2011; April 30, 2012
Index Cross-References: Policy VI-91: Identity Theft Prevention Program
Procedure File Number: 6902
Approved By: Dr. Herman J. Saatkamp, Jr., President

DEFINITIONS

"Identity Theft" is a fraud committed or attempted using the identifying information of another person without authority."

"Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

"Covered Account" is an account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. These accounts include all student accounts or loans that are administered by the University as well as the Perkins Loan Program administered by the service provider Campus Partners.

"Program Administrator" is the individual (or group) designated with primary responsibility for oversight of the Program.

"Identifying information" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person including: name, address, telephone number, social security number, date of birth, driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, student identification number, Internet Protocol address or routing code.

1. PURPOSE:

To ensure compliance with the Federal Trade Commission (FTC) Regulation 16 CFR 681.2, by establishing an Identity Theft Prevention Program designed to reasonably detect, prevent and mitigate identity theft in connection with the opening of a Covered Account or an existing Covered Account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

a. Identify relevant Red Flags for new and existing Covered Accounts offered or maintained and incorporate those Red Flags into the Program;

b. Detect Red Flags that have been incorporated into the Program;

c. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and

d. Ensure the Program is updated periodically to reflect changes in risks to students and to the safety and soundness of the University from identity theft.

2. BACKGROUND:

Regulations promulgated in furtherance of the Fair and Accurate Credit Transactions Act of 2003 require institutions that hold certain Covered Accounts (accounts for which a person makes repeat payments) as defined by the Act to create and implement a program for the prevention of identity theft as relates to such accounts. The administration of Stockton University has determined that certain student accounts would be considered Covered Accounts. Additionally, one service provider account administered by Campus Partners is a Covered Account. Accordingly, the University has taken appropriate steps to become compliant with the regulations.

3. PROCEDURE:

A. IDENTIFICATION OF RED FLAGS

Each area of the University that opens or otherwise handles or manages Covered Accounts, should identify red flags that pertain to those covered accounts. The Program shall include relevant Red Flags from the following categories as appropriate:

i. Alerts, notifications, or warnings received from consumer reporting agencies or service providers, such as fraud detection services;

   a. Report of fraud accompanying a credit report

   b. Notice or report from a credit agency of a credit freeze on an applicant.

   c. Notice or report from a credit agency of an active duty alert for an applicant.

d. Receipt of notice of address discrepancy in response to a credit report request.

e. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

ii. Presentation of suspicious documents

a. Identification document that appears altered, forged or inauthentic.

b. Identification document on which a person's photograph or physical description is not consistent with the person presenting the document.

c. Other document with information that is not consistent with existing student information.

d. Application for service that appears to have altered or forged.

iii. Presentation of suspicious personal identifying information

a. Identifying information that is inconsistent with other information such as inconsistent birth dates, address not matching address on a loan application or photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification.

b. Identifying information presented that is consistent with fraudulent activity such as in invalid phone number or fictitious billing address, social security number presented that is the same as one given by another student, an address or phone number that is the same as that of another person.

c. A person fails to provide complete personal identifying information on an application when reminded to do so.

d. A person's identifying information is not consistent with the information that is on file for the student.

iv. Suspicious activity related to a Covered Account

a. Change of address for an account followed by a request to change the student's last name.

b. Payments stop on an otherwise consistently up-to-date account.

c. Account is used in a way that is not consistent with prior use.

d. Mail sent to the student is repeatedly returned as undeliverable.

e. Notice to the University that the student is not receiving mail sent by the University.

f. Notice to the University that an account has unauthorized activity.

g. Breach of the University's computer system security.

h. Unauthorized access to or use of student account information.

v. A request made from a non-University issued e-mail account;

vi. A request to mail something to an address not listed on file;

vii. Notice from a student, victims of identity theft, law enforcement authorities, or other persons that the University has opened or is maintaining a fraudulent account/loan for a person engaged in Identity Theft.

B. DETECTION OF RED FLAGS

University personnel need to take into consideration and detect red flags in connection with the opening of Covered Accounts/Loans and working with existing Covered Accounts.

a. Student Enrollment/Employee accounts

In order to detect Red Flags associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account.

i. Obtain identifying information such as name, date of birth, academic records, home address or other identification; and

ii. Verify the student's identity at the time of issuance of a student identification card.

b. Existing Accounts

In order to detect Red Flags for an existing Covered Account, University personnel will take the following steps to monitor transactions on the account;

i. Verify the identification of student or employee if they request information in either person, via telephone or e-mail.

ii. Verify the validity of change of billing address requests.

iii. Verify changes in banking information for billing and payment purposes.

c. Consumer ("Credit") Report Requests-Certain Employment Positions

In order to detect any of the Red Flags identified above for an employment position for which a credit or background report is sought, the University will:

i. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and

ii. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

iii. If any information obtained may affect candidacy for the position, follow the University's for pre-employment background checks.

C. RESPONSE

If a Red Flags is detected, personnel should take action to prevent and/or mitigate identity theft. The appropriate responses for the relevant Red Flags are as follows:

i. Monitor a Covered Account for evidence of identity theft;

ii. Deny access to the Covered Account until other information is available to eliminate the red flag, or close the existing Covered Account;

iii. Contact the student and/or provide student with new student identification number;

iv. Change any passwords, security codes or other security devices that permit access to a Covered Account;

iv. Reopen a Covered Account with a new account number or not open a new Covered Account;

v. Notify program administrator for determination of the appropriate step(s) to take;

vi. Notify Vice President for Administration and Finance or Provost to determine appropriate steps to take which may include informing law enforcement that Identity Theft is believed to have occurred ; or

vii. Determine no response is warranted under the particular circumstances.

D. PROTECTING IDENTIFYING INFORMATION

The University will take the following steps with respect to its internal operating procedures to protect identifying information:

i. Ensure the University's website is secure or provide clear notice that the website is not secure;

ii. Ensure complete and secure destruction of paper documents and computer files containing identifying information when such documents or files are no longer needed;

iii. Ensure that office computers with access to Covered Account information are password protected;

iv. Avoid use of social security numbers and allow access to social security numbers to very limited number of staff that have been approved by the Program Administrator;

v. Ensure computer virus protection is up to date;

vi. Require and keep only the kind of information that is necessary for University purposes.

vii. Require all notebook computers, flash drives or removable disk drives acquired by the University for administrative purposes to be equipped and configured to automatically encrypt administrative data.

4. OVERSIGHT OF THE PROGRAM

Responsibility for developing, implementing and updating this program lies with the Vice President for Administration and Finance, the Provost or their designee who shall be the Program Administrators. The Program Administrator or designee(s) will be responsible for the Program and oversight of the Program shall include:

a. Assignment of specific responsibility for implementation of the Program and ensuring appropriate training of University's staff in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected;

b. Reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft;

c. Determining which steps of prevention and mitigation should be taken in particular circumstances;

d. Review of reports prepared by staff regarding compliance; and

e. Approval of material changes to the Program as necessary to address changing risks of identity theft.

f. The Program Administrator will review all requests by staff requesting access to the Social Security Numbers of either students or staff members.

5. STAFF TRAINING AND REPORTS

University staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

a. University staff will be trained as necessary to effectively implement the Program;

b. University staff is expected to notify the Program Administrator once they become aware of an incident of identity theft or of the University's failure to comply with this program.

Reports shall be prepared as follows:

a. The Program Administrator will report to the President's Cabinet at least annually on compliance by the University with the Program beginning December 2011.

b. The report shall address material matters related to the Program and evaluate issues such as:

   i. 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;

   ii. Service provider agreements;

   iii. Significant incidents involving identity theft and management's response; and

   iv. Recommendations for material changes to the Program.

6. OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The University shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more Covered Accounts.

a. Require that service providers have such policies and procedures in place;

b. Require that service providers review the University's Program and report any Red Flag to the University employee with primary oversight of the service provider relationship.

7. UPDATING THE PROGRAM

The Program shall be reviewed and updated periodically by the Program Administrator to reflect changes in risks to students or to the safety and soundness of the University from identity theft based on factors such as:

a. The experience of the organization with identity theft;

b. Changes in methods of identity theft;

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

d. Changes in the types of accounts that the organization offers or maintains;

e. Changes in the University's business arrangements with other entities.

Approval History:

	Date
President	4/30/12