

# STOCKTON UNIVERSITY

## PROCEDURE

### Identity Theft Prevention Program

Procedure Administrator: Risk Manager

Authority: N.J.S.A. 18A:64-8; Fair and Accurate Credit Transactions Act of 2003, 16 CFR 681

Effective Date: May 6, 2009; February 16, 2011; April 30, 2012; August 10, 2023

Index Cross-References: Policy VI-91: Identity Theft Prevention Program

Procedure File Number: 6902

Approved By: Dr. Joe Bertolino, President

- 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.

### III. BACKGROUND:

Regulations promulgated in furtherance of the Fair and Accurate Credit Transactions Act of 2003 require institutions that offer or maintain certain Covered Accounts to create and implement a program for the prevention of identity theft related to such accounts. The administration of Stockton University has determined that certain student accounts administered by the University, as well as an account administered by a service provider, would be considered Covered Accounts.

### IV. PROCEDURE:

#### A. IDENTIFICATION OF RED FLAGS

Each area of the University that opens or otherwise maintains or manages Covered Accounts should identify Red Flags pertaining 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, including:
  - 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 a notice of address discrepancy in response to a credit report request; or
  - e. Indication from a credit report of activity that is inconsistent with an

- iii. Presentation of suspicious personal Identifying Information, including:
  - a. Identifying Information that is inconsistent with other information e.g., inconsistent birth dates, address not matching address on a loan application, or a photograph or physical description that is inconsistent with the appearance of the student presenting the identification;
  - b. Identifying Information that is consistent with fraudulent activity e.g., an invalid phone number or fictitious billing address, a social security number that has been provided by another student, or an address or phone number that is the same as that of another person;
  - c. Failure to provide complete personal Identifying Information on an application when reminded to do so; or
  - d. Identifying Information that is inconsistent with the information on file for the student.
- iv. Suspicious activity related to a Covered Account, including:
  - a. Change of address for an account followed by a request to change 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. security; or
  - 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

b. Verify the individual identity at the time of issuance of a University identification card.

ii. Existing Accounts

In order to





- D. Changes in the types of accounts that the organization offers or maintains; and
- E.