3357:13-17-52 Identity Theft Protection Policy

(A) Purpose

(1) The purpose of this policy is to establish an Identity Theft Prevention Program designed to 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. In accordance with the Federal Trade Commission's Red Flags Rule, the Program shall include reasonable guidelines and procedures to:

(a) Identify relevant red flags for covered accounts it offers or maintains 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 creditor from identity theft.

(2) The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

(B) Definitions

(1) Identify theft means fraud committed or attempted using the identifying information of another person without authority.

(2) Covered account means:

(a) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

(b) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to students or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

(3) Red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

(C) Identification of Relevant Red Flags

The Program shall include relevant red flags from the following categories as appropriate:

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents, such as appearing altered or forged;

(3) The presentation of suspicious personal identifying information, such as a photograph or physical description on the identification that is not consistent with the appearance of the student presenting the identification;

(4) A request to mail something to an address not listed on file;

(5) The unusual use of, or other suspicious activity related to, a covered account; and

(6) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

(D) Detection of Red Flags

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(1) Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and

(2) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

(E) Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags may include:

(1) Monitoring a covered account for evidence of identity theft;

(2) Denying access to the covered account until other information is available to eliminate the red flag, or close the existing covered account;

(3) Contacting the student;

(4) Changing any passwords, security codes or other security devices that permit access to a covered account;

(5) Reopening a covered account with a new account number;

(6) Notifying Campus Services or law enforcement; or

(F) Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

(1) The experiences of the organization with identity theft;

(2) Changes in methods of identity theft;

(3) Changes in methods to detect, prevent and mitigate identity theft;

(4) Changes in the types of accounts that the organization offers or maintains;

(5) Changes in the College's business arrangements with other entities.

(G) Oversight of the Program

The Treasurer is responsible for the Program and its oversight. The Treasurer shall be responsible for assignment of specific responsibility for implementation of the Program and ensuring appropriate training of College staff in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. The Treasurer shall determine which steps of prevention and mitigation should be taken in particular circumstances; and approve material changes to the Program as necessary to address changing risks of identity theft.

(H) Oversight of Service Provider Arrangements

The College 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.

Effective: March 23, 2011
Expires: 3/23/16
Review Dates: 3/23/11