3354:2-11-05 Identity Theft Protection.

(A) Purpose

1) The College creates, obtains, and stores personally-identifiable financial and other sensitive information, and desires to ensure appropriate measures are taken to prevent identity theft involving such information. Therefore, the College shall maintain an active Identity Theft Prevention Program in accordance with Federal Trade Commission regulations enacted under 16 CFR 681.2 (often referenced as the "Red Flag Rule").

2) The Controller and Bursar shall serve as "Compliance Officer" leading development, implementation, and oversight of the identity theft program.

(B) Definitions

1) "Covered accounts" are the College's tuition loan plans, emergency loans, Perkins loans, Nursing loans, Federal Family Education Loans (FFEL), and employee computer loans, and any other future accounts and/or transaction credits into the future.

2) "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 without limitation: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, student identification number, employee identification number, computer's internet protocol address, and routing code.

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

4) "Red Flag" means a "pattern, practice, or specific activity that indicates the possible existence of identity theft."

(C) Identifying Red Flags

1) The program should identify red flags for covered accounts and incorporate those red flags into the program.

a. The program should incorporate the following risk factors in identifying relevant red flags for covered accounts:

i. The types of covered accounts offered or maintained by the College.

ii. The methods provided by the College to open covered accounts.

iii. The methods provided by the College to access covered accounts.

iv. The College's experience, if any, with identity theft.

b. The program should incorporate appropriate red flags from relevant experiences and sources, including without limitation:

i. Incidents of identity theft previously experienced.

ii. Methods of identity theft that reflect changes in risk.

iii .Regulatory or professional guidance.

c. As appropriate, the program shall include relevant red flags from the following categories of risk factors:

i. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.

ii. The presentation of suspicious documents.

iii. The presentation of suspicious personal identifying information.

iv. The unusual use of, or other suspicious activity related to, a covered account.

v. Notice from customers, employees, students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

(D) Detecting and Responding to Red Flags

1) The College's Identity Theft Prevention Program should address the detection of red flags in connection with the opening of new covered accounts and existing covered accounts.

a. The program should provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The responses should be commensurate with the degree of risk posed, and may include:

i. Monitoring a covered account for evidence of identity theft.

ii. Denying access to the covered account until other information is available to eliminate the red flag, or close the existing covered account.

iii. Contacting the student, former student, current employee, or former employee.

iv. Changing any passwords, security codes or other security devices that permit access to a covered account.

v. Reopening a covered account with a new account number.

vi. Notifying a College administrator and the relevant Compliance Officer (Controller and Bursar).

(E) Updating the Identity Theft Prevention Program

1) The College should periodically, and at least annually, update the program in accordance with appropriate factors, which may include:

a. The experiences 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 business arrangements of the organization, including without limitation, service provider agreements.

(F) Methods of Administering the Program

1) In administering the Identity Theft Prevention Program, the Compliance Officer shall be responsible for:

a. Training of College staff on the program.

b. Requiring and reviewing reports on compliance with this program. The Identity Theft Program should include appropriate details about this reporting process.

c. Leading prevention and mitigation efforts in particular circumstances.

d. Monitoring and ensuring College compliance with the Identity Theft Prevention Policy and Program.

e. Overseeing the activities of service providers performing activities related to covered accounts to ensure that such activities are conducted pursuant to reasonable policies and programs designed to detect, prevent, and mitigate the risk of identity theft.

Replaces: 3354:2-11-05

Effective: 02/03/2011

CERTIFIED ELECTRONICALLY

Certification

03/10/2015

Date

Promulgated Under: 111.15
Statutory Authority: 3354
Rule Amplifies: 3354
Prior Effective Dates: 2/3/2011