SOUTH DAKOTA BOARD OF REGENTS

Policy Manual

SUBJECT: Identity Theft Prevention

NUMBER: 5.10

A. PURPOSE

To establish a written program to detect, prevent, and mitigate instances of identity theft on financial accounts.

B. DEFINITIONS

1. **Fair and Accurate Credit Transactions Act**: A federal consumer-rights law to reduce the risk of identity theft by regulating how consumer account information is handled.

C. POLICY

The Board of Regents and its institutions maintain financial accounts that permit multiple payments or transactions. As a result of maintaining these accounts, the Board of Regents and its institutions are subject to regulations commonly referred to as Red Flag Rules, governed by the Fair and Accurate Credit Transactions Act. The regulations serve to detect, prevent, and mitigate instances of identity theft on financial accounts.

1. **Oversight and Review**

   1.1. The Board of Regents' universities will develop and maintain an identity theft prevention program. The program will include procedures for detecting, preventing, and mitigating instances of identity theft. The program will be overseen by the financial vice presidents of the institutions with an annual report tracking and reporting all significant red flag activity including incidents, resolutions and program updates to be reviewed by the Business Affairs Council annually. The Red Flags Program will undergo annual scrutiny; based on current business realities and new developments, it will be revised as appropriate.

2. **Red Flags Program**

   2.1. Red flags equate to warning signs that signal identity theft. The crux of this program entails discerning and reacting to five types of red flags:

      2.1.1. Alerts, notifications, and warnings provided by consumer reporting agencies in response to requests for credit reports of potential employees:

      - Report of fraud

      - Notice/report of a credit freeze

- Notice/report of an active duty alert

- Notice of address discrepancy

2.1.2. Suspicious documents:

- Identification document or card that appears to be forged, altered, or inauthentic

- Identification card on which the student's photograph or physical description is inconsistent with person presenting card

- Other document information that is incongruent with existing student data

2.1.3. Suspicious personally identifying information:

- Presentation of identifying information that is inconsistent with other information provided by the student (example: birth dates do not match)

- Presentation of identifying information that conflicts with that on file or available through other sources

- Submission of information that points to fraudulent activity (examples: invalid phone numbers and fictitious addresses)

- Provision of social security number that is identical to that already provided by another student

- Failure to provide complete personal identifying information despite reminders to do so

2.1.4. Suspicious activity related to covered accounts:

- Payments stop on a typically up-to-date loan account

- Mail sent to the student is repeatedly returned as undeliverable

- Communication from a student that he/she is not receiving mail sent by the university

- Breach in the university's computer system security

- Unauthorized access to student account information

2.1.5. Notices from students and law enforcement authorities regarding possible identity theft connected to covered accounts:

- Notification from a student that his/her identity has been stolen

- Warning shared by a victim or law enforcement personnel that the university is conducting business (specifically, maintaining a covered account) with an identity thief

2.2. Following detection, university staff will assess degree of risk imposed by the particular red flag and provide appropriate follow-up action as merited:

2.2.1. Continue monitoring covered account for additional evidence of identity theft.

2.2.2. Contact applicant for whom credit check was conducted.

2.2.3. Change any passwords or other security devices that permit access to covered accounts.

2.2.4. Attach a privacy hold to impacted student's account.

2.2.5. Following consultation with System Banner Administrator, provide student with new identification number.

2.2.6. Inform immediate supervisor and Campus Program Administrator.

2.2.7. Notify law enforcement personnel.

2.3. Not all red flags will trigger follow-up action; in certain scenarios, staff members may apply prior knowledge and determine that no further action is warranted.

3. Service Provider Arrangements

3.1. When Regental universities choose to use a third party for financial transactions that fall under the Fair and Accurate Credit Transactions Act regulations, such as contracting for repayment of Perkins Loans, the campus administrator is responsible to insure that the service provider of choice performs its activities in accordance with the Red Flags Rules.

FORMS / APPENDICES:

None

SOURCE:

BOR August 2009; October 2018; August 2020 (Clerical); October 2023 (Clerical).