INFORMATION SECURITY 2.25070 BP
Identity Theft Prevention, Detection, and Mitigation BOARD POLICY

PURPOSE

The Board authorizes the Chancellor to develop, maintain and update an Identity Theft Prevention Program ("Program") to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account.

OBJECTIVE

The Program will: 1) Identify the red flags of identity theft that may occur in day-to-day operations; 2) Detect red flags; 3) Prevent, mitigate, and respond to red flags; and 4) Update and provide continued administration of the Program.

APPLICABILITY

This Program covers all devices that have MCC data including those by vendors hosting MCC data. This Program applies to all employees.

This Program is not intended to supersede any existing MCC policy that provides more specific requirements for safeguarding certain types of data, including the definition of directory information under the Family Educational Rights and Privacy Act (FERPA).

DEFINITIONS

"Account" is any continuing relationship between MCC and an account holder that permits the account holder to obtain a product or service for personal, family, household, or business purposes.

"Account Holder" is a student, employee, retired employee, or other person that has a covered account held by or on behalf of MCC.

"Covered Account" is:

1. Any account MCC offers or maintains primarily for personal, family, household or business purposes, that is designated to permit multiple payments or transactions. This account may be maintained by MCC or by a third party vendor on behalf of MCC.

2. Any other account MCC offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of MCC from Identity Theft.

"Identity Theft" is defined as fraud committed using the identifying information of another person to obtain a thing of value including money, credit, items, or services, such as education services to which the individual is not entitled to.

"Identifying information" is defined as 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, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

"Red Flag" is a pattern, practice, or specific activity in connection with an MCC covered account that indicates the possible existence of Identity Theft.

RESPONSIBLE PARTY

The Chancellor appoints the Chief Information Security Officer or designee as the responsible party for maintaining the Program and providing reports. The responsible party may incorporate any policies and regulations that promote the purpose of the Program. The responsible party may also incorporate information security tools to assist with implementation of the Program.

APPROVALS

The Chancellor shall approve the written Identity Theft Prevention, Detection, and Mitigation Program.

PROGRAM REQUIREMENTS

The Program shall include at a minimum the following:

1. A list of all departments identified as holding covered accounts applicable to this Program.
2. Identify the officer or employee of departments identified as holding covered accounts as the responsible party for ensuring the are in compliance with the Program and Red Flags Rules.
3. Identify "Red Flags" associated with covered accounts within a department.
4. Implement practices to detect the presence of "Red Flags" in connection with all covered accounts the Program identifies.
5. Practices for response to detected "Red Flags" to prevent and mitigate identity theft.
6. Timeframes for conducting periodic risk assessments to identify responsibility for covered accounts for incorporation into the Program.
7. Periodic review and update of the Program to reflect changes in risk associated with identity theft.
8. Make periodic reports to appropriate Officer to ensure compliance.
9. Periodic training of all MCC employees necessary to implement and enforce the Program.