Policy Number: 601.1
Policy: Identity Theft Prevention Program
Effective Date: October 5, 2011
Revision Date: December 21, 2023
Approved by: Vice Chancellor for Administration and Finance

POLICY STATEMENT:

100.00 Introduction and Purpose
Identity thieves use personally identifiable information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. In response, the Federal Trade Commission published the Red Flags Rule. This rule requires financial institutions and creditors to implement a program to detect, prevent, and mitigate identity theft. Since Montana State University Billings (MSU Billings) regularly extends, renews, or continues credit, this rule applies. Pursuant to this rule and to prevent identity theft at Montana State University, its campuses collaboratively developed this program.

110.00 Definitions

110.10 Covered account

1. 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, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
3. The following are examples of covered accounts: student accounts, short-term loans, and certain payroll accounts.

110.20 Identity theft is a fraud committed or attempted using the personally identifiable information of another person without authority.

110.30 Red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

110.40 Personally identifiable information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: name, address, telephone number, student identification number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, and employer or taxpayer identification number.

POLICY: Sections 120.00 and 130.00

120.00 Program Administrators Responsibilities
The most senior financial administrator at each of the campuses shall be its respective identity theft prevention program administrator. Responsibilities of the program administrator follow:

1. Ensure that units containing covered accounts at their respective campuses have implemented identity theft prevention procedures.
2. Obtain, review and compile unit's reports of the discovery of identity theft.
3. Ensure that training is available for their respective campuses' units.
4. Evaluate the program annually to determine whether all aspects of the Program are up to date and applicable in the current business environment. Aspects to consider include assessment of accounts

covered by the Program; revision, replacement or addition of Red Flags and other potential updates that may be deemed necessary based on additional experience with the Program.

5. The campuses' Program Administrators will collaboratively review and approve material changes to this written Program as necessary to address changing identity theft risks.

130.00 Requirements of the Identity Theft Prevention Program

The dean, director, department head or other supervisor of a unit containing a covered account is responsible for implementing and documenting identity theft prevention procedures, including the following elements:

1. Identifying Relevant Red Flags
2. Detecting Red Flags
3. Preventing and Mitigating Identity Theft
4. Reporting the Discovery of Identity Theft to the Program Administrator
5. Training Staff on Identity Theft Prevention Procedures
6. Oversight of Service Provider Arrangements

REFERENCES:

BOR Policy 960.1; BOR Policy 1300.1; Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA); Section 615(e) of the Fair Credit Reporting Act (FCRA); and the Federal Trade Commission CFR Parts 681.2 and 681.3; University of Montana Identity Theft Prevention Program