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

PROCEDURE:

I. Identifying Relevant Red Flags

In order to identify relevant Red Flags, units containing covered accounts must consider the following:

A. Types of covered accounts they offer and maintain,
B. Methods they provide to open covered accounts,
C. Methods they provide to access covered accounts, and
D. Previous experiences with identity theft.
E. Examples of Potential Red Flags (listed in Appendix)

II. Detecting Red Flags

Units containing covered accounts must implement procedures to address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as:

A. Opening Covered Accounts

Any individual attempting to open a covered account will be required to provide personally identifiable information in order to verify their identity prior to the establishment of the account.

B. Existing Covered Accounts

In order to change information on an existing covered account, it will be necessary to verify the individual's identity and to verify the validity of all change of address requests. For example:

1. Verify the identification of individuals if they request information (in person, via on-line access, via telephone, via facsimile, or via e-mail);
2. Verify the validity of requests to change billing addresses by mail or e-mail and provide the account holder a reasonable means of promptly reporting incorrect billing address change; and
3. Verify changes in banking information given for billing or payment purposes.

III. Preventing and Mitigating Identity Theft

In the event that a unit detects any Red Flags, it shall take one or more of the following steps, depending upon the degree of risk posed by the Red Flag(s):

A. Monitoring the account for evidence of identity theft
B. Contacting the customer
C. Changing passwords or security codes and PIN's
D. Reopening an account with a new account number
E. Not opening a new account
F. Closing an existing account
G. No collection on an account
H. Notifying law enforcement; or
I. Determining that no response is warranted under the particular circumstances.

IV. Reporting the Discovery of Identity Theft to the Program Administrator

In the event that identity theft is discovered, the unit shall report the incident to the Program Administrator as soon as practicable for assistance with determining steps for preventing and mitigating identity theft as well as for assisting the Program Administrator in its report compilation responsibilities.

V. Training for Identity Theft Prevention Procedures

The dean, director, department head or other supervisor of a unit containing a covered account is responsible for ensuring that employees who they determine to be in a position to detect Red Flags receive training on identity theft prevention procedures.

VI. Oversight of Service Provider Arrangements

If a unit engages a service provider to perform an activity in connection with one or more covered accounts, the dean, director, department head or other supervisor shall take the following steps to ensure the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

A. Require, by contract, that service providers have such policies and procedures in place; and

B. Require, by contract, that service providers certify their compliance with applicable FTC regulations, report any Red Flags to the respective campuses' Program Administrator and to take appropriate steps to prevent or mitigate identity theft.

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