Identity Theft Prevention Program (DRAFT)

Subject:	**Financial Affairs**
Revised:	**N/A**
Effective date:	**TBD**
Review date:	**Annually TBD**
Responsible Party:	**MSU-Bozeman Vice President for Administration & Finance**

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 (MSU) regularly extends, renews, or continues credit, this rule applies. Pursuant to this rule and to prevent identity theft at MSU, its campuses collaboratively developed this program.

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]

110.00 Definitions

110.10 Covered accounts include any account that involves or is designed to permit multiple payments or transactions. Every new and existing account that meets the following criteria is covered by this Program:

1. Business and personal accounts for which there is a reasonably foreseeable risk of identity theft; or

2. A business or personal account for which there is a reasonably foreseeable risk to MSU account holders or to the safety or soundness of the university from identity theft, including financial, operational, compliance & liability or reputational risks.

The following are examples of covered accounts: Student Accounts, Short-Term Loans, Certain Payroll Accounts and Campus Based Identification Cards.

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.

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:

130.10 Identifying Relevant Red Flags
130.20 Detecting Red Flags
130.30 Preventing and Mitigating Identity Theft
130.40 Reporting the Discovery of Identity Theft to the Program Administrator
130.50 Training Staff on Identity Theft Prevention Procedures
130.60 Oversight of Service Provider Arrangements

130.10 Identifying Relevant Red Flags

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

1. Types of covered accounts they offer and maintain,
2. Methods they provide to open covered accounts,
3. Methods they provides to access covered accounts, and
4. Previous experiences with identity theft.

MSU identifies potential Red Flags in the appendix of this Program.

130.20 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:

130.22 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.

130.24 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.

130.30 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):

1. Monitoring the account for evidence of identity theft
2. Contacting the customer
3. Changing passwords or security codes and PIN's
4. Reopening an account with a new account number
5. Not opening a new account
6. Closing an existing account
7. No collection on an account
8. Notifying law enforcement; or
9. Determining that no response is warranted under the particular circumstances.

130.40 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.

130.50 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.

130.60 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.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. 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.

Identity Theft Prevention Program Appendix
Potential Red Flags

Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personally Identifiable Information

6. Personally identifying information provided is inconsistent when compared against external information sources used by the University. For example:
    a. The address does not match any address in the consumer report; or
    b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
7. Personally identifying information provided by the customer is not consistent with other personally identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
8. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example:
    a. The address on an application is the same as the address provided on a fraudulent application; or
    b. The phone number on an application is the same as the number provided on a fraudulent application.
9. Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University. For example:
    a. The address on an application is fictitious, a mail drop, or a prison; or
    b. The phone number is invalid, or is associated with a pager or answering service.
10. The SSN provided is the same as that submitted by other persons opening an account or other customers.
11. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
12. The person opening the covered account or the customer fails to provide all required personally identifying information on an application or in response to notification that the application is incomplete.
13. Personally identifying information provided is not consistent with personally identifying information that is on file with the University.

14. When using challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

15. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
16. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
    a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
    b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
17. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    a. Nonpayment when there is no history of late or missed payments;
    b. A material increase in the use of available credit;
    c. A material change in purchasing or spending patterns;
    d. A material change in electronic fund transfer patterns in connection with a deposit account; or
    e. A material change in telephone call patterns in connection with a cellular phone account.
18. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
19. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
20. The University is notified that the customer is not receiving paper account statements.
21. The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the University

22. The University is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Other Red Flags

23. You may identify other Red Flags not listed that may be more applicable to your situation.