Federal Trade Commission Red Flags Identity Theft Prevention Program

Subject: Financial Affairs

Revised: April 6, 2024

Effective Date: October 5, 2011

Review Date: April 2027

Responsible Party: MSU-Bozeman Vice President for Administration & Finance

Scope

This policy applies to Montana State University including the affiliate campuses:

- Montana State University Billings including City College
- Montana State University Northern
- Great Falls College, Montana State University
- All other Montana State University campuses including Extension, Agricultural Experiment Stations, and Gallatin College

For the purpose of this policy, the acronym “MSU” refers to all campuses listed above.

100.00 Introduction and Purpose

MSU regularly manages accounts such as direct deposit, vendor/individual payments, and occasionally short-term loans. Establishing these accounts requires the use of personally identifiable information. MSU strives to keep personally identifiable information confidential and secure.

To mitigate the possibility of identity theft, the Federal Trade Commission (FTC) has published the Red Flags Rule. This rule requires financial institutions and creditors to implement a program to detect, prevent, and mitigate identity theft. Pursuant to the Red

Flags 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, Identity Theft Rules https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681#681.1;

200.00 Definitions

210.00 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 students or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The following are examples of covered accounts: student accounts, short-term loans, and certain payroll accounts.

220.00 Identity theft

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

230.00 Red flag

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

240.00 Personally identifiable information

Personally Identifiable Information (PII) 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/employee identification number, NetID, 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.

300.00 Policy

310.00 Responsible Parties

The Vice President for Administration and Finance or the most senior financial administrator at each of the campuses will be the responsible officers. The Identity Theft Prevention Committee (ITPC), comprised of one representative from University Compliance, University Business Services, University Information Technology, and University Human Resources, shall be responsible for the administration and monitoring of the Identity Theft Prevention Program. When considering reports from affiliate campuses, the responsible officer from that campus will be present.

Responsibilities of the responsible parties:

1. The administrator will ensure that units containing covered accounts at their respective campuses have implemented identity theft prevention procedures.
2. The ITPC will obtain, review and compile unit's reports of the discovery of identity theft.
3. The administrator will ensure that training is available for campuses units who manage covered accounts.
4. In consultation with the officer, the ITPC will 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. In consultation with the officer andthe administrators, the ITPC will collaboratively review and approve material changes to this written Program as necessary to address changing identity theft risks.

320.00 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 the Identity Theft Prevention Program procedures including:

- 410.00 Identifying Relevant Red Flags

- 420.00 Preventing, Responding, and Mitigating Identity Theft
- 421.00 Detecting Red Flags
- 422.00 Opening Covered Accounts
- 423.00 Existing Covered Accounts
- 424.00 Reporting the Discovery of Red Flags and Identity Theft
- 425.00 Staff training compliance for Identity Theft Prevention Procedures
- 426.00 Oversight of Service Provider Arrangements

400.00 Procedures

410.00 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 provide to access covered accounts, and
4. Previous experiences with identity theft.

Note: Potential Red Flags are identified later in the Program.

420.00 Preventing, Responding to, and Mitigating Identity Theft

421.00 Detecting Red Flags

Units managing covered accounts must implement procedures to keep confidential information safe and secure. Red Flags in connection with the opening of covered accounts and existing covered accounts, such as:

422.00 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.

423.00 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.

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 account owner
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

424.00 Reporting the Discovery of Red Flags and Identity Theft

In the event that red flags are identified, or identity theft is discovered, the unit shall report the incident to the ITPC as soon as practicable for assistance with determining steps for preventing and mitigating identity theft. Other offices, depending on the situation, may need to be informed as well. Examples include Safety and Risk Management, Audit Services, University Police Department, University Compliance, University Business Services, or Human Resources.

425.00 Training for Identity Theft Prevention Procedures

Training for identity theft prevention and procedures will be provided by Montana State University to appropriate individuals. Employees who work directly with Covered Accounts will take training annually, and compliance with the training will be the responsibility of the employee's director or department head.

426.00 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, working with MSU Procurement and Contract Services, 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.

500.00 Appendix 1: Potential Red Flags

510.00 Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or credit alert is included with a consumer report.
2. A notice of credit freeze on a consumer report is provided from a consumer reporting agency.
3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a consumer.

520.00 Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant, student or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account, student or customer presenting the identification.
8. 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.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

530.00 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 account owner is not consistent with other personally identifying information provided by the account owner. 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 an answering service.
10. The SSN provided is the same as that submitted by other persons opening an account or others.
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 others.
12. The person opening the covered account, the student 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, the student or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

540.00 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 account owner 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 account owner is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account owner's covered account.
20. The University is notified that the account owner is not receiving paper account statements.
21. The University is notified of unauthorized charges or transactions in connection with a account owner's covered account.

550.00 Notice from Students, 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 student, 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.

560.00 Other Red Flags

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