# Red Flags Departmental Procedures for [INSERT DEPT]

|  |  |
| --- | --- |
| **Subject:** | Federal Trade Commission Red Flags Identity Theft Prevention Program Department Procedures |
| **Effective Date:** | [INSERT DATE] |
| **Report Red Flags to:** | The Identity Theft Prevention Committee (ITPC) [financialservices@montana.edu](mailto:financialservices@montana.edu) |



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.

This procedures document outlines the steps the employees in this department need to take to mitigate and respond to identity theft red flags.

## Covered Accounts

A covered account is an account which falls under the Red Flags Rule and are the accounts which are most likely to uncover Red Flags.

At MSU these can be:

* Accounts primarily for personal, family, or household purposes that allow multiple payments or transactions (e.g., credit cards, loans, utility accounts).
* Accounts with foreseeable risks of identity theft to students or account owners, including operational, compliance, reputation, or litigation risks.

A few examples at MSU:

* Student accounts
* Short-term loans
* Certain payroll accounts

Examples in our department:

* [Add specific example]
* [Another example]

## Procedures for monitoring Red Flags

### 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.

### Existing Covered Accounts

Verify the individual’s identity and 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.

[Add other department procedures for monitoring]

## Workplace Implementation

Our workplace must adhere to the FACTA and GLBA regulations regarding Personally Identifiable Information (PII) and Nonpublic Personal Information (NPI.)

### Clean desk policy

Desks must be kept clean and free of visible or easily accessible information or passwords relating either to PII/NPI or gaining access to accounts containing PII and NPI.

### Shred documents containing PII or NPI

Documents not currently in use or securely stored must be shredded. If the department uses a shred box, the box must be kept securely locked.

### Computers that interact with NPI cannot accept USB thumb drives

Any desktops, laptops or other devices interacting with NPI cannot have USB/thumb drives allowed to access it. Contact MSU UIT if you need to update any devices.

## When a Red Flag is Detected

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

### First: Report the Discovery of the Red Flag or Identity Theft

In the event that red flags are identified, or identity theft is discovered, this department shall report the incident to the supervisor and the Identity Theft Prevention Committee (ITPC) as soon as practicable for assistance with determining steps for preventing and mitigating identity theft by emailing [financialservices@montana.edu](mailto:financialservices@montana.edu).

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.

## Oversight of Service Provider Arrangements

A service provider performing an activity in connection with one or more covered accounts, we 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.

Contact [financialservices@montana.edu](mailto:financialservices@montana.edu) when considering these contracts along with Procurement Services.

## Potential Red Flags

### Red Flags specific to this department

* [insert]
* [insert]

### 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.

### 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, student 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, student 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

1. Personally identifying information provided is inconsistent when compared against external information sources used by the University. For example:
   1. The address does not match any address in the consumer report; or
   2. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
2. 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.
3. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example:
   1. The address on an application is the same as the address provided on a fraudulent application; or
   2. The phone number on an application is the same as the number provided on a fraudulent application.
4. 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:
   1. The address on an application is fictitious, a mail drop, or a prison; or
   2. The phone number is invalid, or is associated with an answering service.
5. The SSN provided is the same as that submitted by other persons opening an account or others.
6. 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.
7. 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.
8. Personally identifying information provided is not consistent with personally identifying information that is on file with the University.
9. 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.

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

1. 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.
2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
   1. 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
   2. The account owner fails to make the first payment or makes an initial payment but no subsequent payments.
3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
   1. Nonpayment when there is no history of late or missed payments;
   2. A material increase in the use of available credit;
   3. A material change in purchasing or spending patterns;
   4. A material change in electronic fund transfer patterns in connection with a deposit account; or
   5. A material change in telephone call patterns in connection with a cellular phone account.
4. 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).
5. 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.
6. The University is notified that the account owner is not receiving paper account statements.
7. The University is notified of unauthorized charges or transactions in connection with an account owner's covered account.

### 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

1. 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.