IDENTITY THEFT DETECTION, PREVENTION AND MITIGATION PROCEDURES

I. Identifying Relevant Red Flags

Select specific Red Flags to meet your department's situation.

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 Montana Tech, 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 Personal Identifying Information

6. Personal identifying information provided is inconsistent when compared against external information sources used by Montana Tech. 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. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
8. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Montana Tech. 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. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Montana Tech. 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 personal identifying information on an application or in response to notification that the application is incomplete.
13. Personal identifying information provided is not consistent with personal identifying information that is on file with Montana Tech.
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. Montana Tech is notified that the customer is not receiving paper account statements.
21. Montana Tech 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 Montana Tech

22. Montana Tech 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.

II. Detecting Red Flags

Opening Covered Accounts

In order to establish or open a covered account, it will be necessary to obtain personal identifying information about, and verifying the identity of a person opening a covered account. Documentation shall be kept on file by Montana Tech to substantiate the validation of the person's identity when establishing a covered account. For example:

1. Require certain personal identifying information such as name, date of birth, academic records, I-9, home address, or other identification; and
2. Verify the individual's identity at time of issuance of a campus based identification card (review of driver's license or other government-issued photo identification)

Existing Covered Accounts

In order to change information on an existing covered account, it will be necessary to authenticate the customer'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 Red Flag is detected in connection with the opening of a covered account or a change to an existing covered account, management of the department containing the covered account shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag. In determining an appropriate response, Montana Tech should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by Montana Tech to someone fraudulently claiming to represent Montana Tech or to a fraudulent website. Appropriate responses may include the following:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopening a covered account with a new account number;
5. Not opening a new covered account;
6. Closing an existing covered account;
7. Not attempting to collect on a covered account or not selling a covered account to a debt collector;
8. Notifying law enforcement; or
9. Determining that no response is warranted under the particular circumstances.

In the event that identity theft is discovered, it is to be reported to the Business Office immediately.

IV. Implementing the Program

Staff training shall be conducted for all employees and officials for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to Montana Tech or its customers.

University staff responsible for implementing the Identity Theft Prevention Program shall be trained as necessary either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University employees are expected to notify their supervisor once they become aware of an incident of Identity Theft or of the University's failure to comply with the program. Staff responsible for development, implementation, and administration of the program will report to the Program Administrator, at least annually on compliance including the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the program.

To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

V. Reporting on the Program

The department will provide a report to the Executive Committee by May 1st of each year regarding the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for material changes to the Program.