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

APPENDIX: EXAMPLES OF POTENTIAL RED FLAGS

I. 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.

II. Suspicious Personally Identifiable Information

1. 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.
2. 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.
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:
    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.
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:
    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.
5. The SSN provided is the same as that submitted by other persons opening an account or other customers.
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 other customers.
7. 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.
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 or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

III. 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:
    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.
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:
    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.
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 customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
6. The University is notified that the customer is not receiving paper account statements.
7. The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

IV. 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

1. 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.

V. Other Red Flags

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

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