SOUTHWEST
MINNESOTA STATE UNIVERSITY

RED FLAGS IDENTITY THEFT PREVENTION PROGRAM

I. Program Adoption

Southwest Minnesota State University ("SMSU") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Administration of SMSU determined that this Program was appropriate for SMSU and therefore approved this Program on May 13, 2010. Incorporated with this program is the Minnesota State Colleges and Universities, Office of the Chancellor Guidelines—Identity Theft Prevention Program which can be found at https://mnscu.sharepoint.com/sites/finance/sitepages/topic.aspx?topicID=97&state=about

II. Definitions and Program

A. Red Flag Rule Definitions

1) "Identity Theft" is a "fraud committed or attempted using the identifying information of another customer without permission."

2) "Identifying Information" is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific customer. Personal or confidential information includes, but is not limited to, the following items whether stored in electronic or printed format:
    a) Name (maiden name)
    b) Address
    c) Telephone number(s)
    d) Social Security Number or taxpayer identification number
    e) Student or employee identification number
    f) Driver's license
    g) Alien registration or passport number
    h) Customer number
    i) Date of Birth
    j) Computer's Internet Protocol (IP) address
    k) Banking information and routing number
    l) Credit Card number and expiration date.

3) A "Red Flag" is a "pattern, practice or specific activity that indicates the possible existence of Identity Theft."

4) A “Covered Account” includes all student or employee (“customer”) accounts or loans that are administered by the University.

5) “Program Administrator” is the individual designated with primary responsibility for oversight of the program.

B. Fulfilling requirement of the Red Flag Rules

Under the Red Flag Rule, SMSU is required to establish an “Identify Theft Prevention Program” tailored to its size, complexity, and nature of its operation. Each program must contain reasonable policies and procedures to:

1) Identify patterns, practices, or specific activities (“Red Flags”) for new and existing covered accounts that indicate the possible existence of identity theft with regard to new or existing covered account;

2) Detect Red Flags that have been incorporated into the Program;

3) Respond appropriately to any Red Flags that are detected to prevent and mitigate Identify Theft;

4) Ensure that the program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the customer from Identity Theft; and

5) Promote compliance with state and federal laws and regulations regarding identity theft protection.

III. <u>Covered Accounts</u>

SMSU has identified various types of accounts that fall within the definition of a covered account as set forth below:

1) Federal Loans (such as the Perkins Loan Program)

2) Student Short Term Loans

3) Student Accounts

4) Employee Accounts

IV. <u>Identification of Red Flags</u>

In order to identify relevant Red Flags, SMSU considers the types of accounts it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The following Red Flags are potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag is apparent, it should be investigated for verification.

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1) Notice or report from a credit agency of a credit freeze on an applicant;

2) Notice or report from a credit agency of an active duty alert for an applicant; and

3) Receipt of Notice of Dispute from a credit agency.

B. Suspicious Documents

Red Flags

1) Identification document or card that appears to be forged, altered or inauthentic;

2) Identification document or card on which a customer's photograph or physical description is not consistent with the customer presenting the document;

3) Other document with information that is not consistent with existing student or employee information; and

C. Suspicious Personal Identifying Information

Red Flags

1) Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);

2) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);

3) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

4) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5) Social security number presented that is the same as one given by another customer;

6) An address or phone number presented that is the same as that of another customer;

7) A customer fails to provide complete personal identifying information on an application when reminded to do so; and

8) A customer's identifying information is not consistent with the information that is on file for the student.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1) Change of address for an account followed by a request to change the customer's name;

2) Payments stopped on an otherwise consistently up-to-date account;

3) Account used in a way that is not consistent with prior use;

4) Mail sent to the customer is repeatedly returned as undeliverable;

5) Notice to the University that a customer is not receiving mail sent by the University;

6) Notice to the University that an account has unauthorized activity;

7) Breach in the University's computer system security; and

8) Unauthorized access to or use of a customer's account information.

E. Alerts from Others

Red Flag

1) Notice to the University from a student, employee, Identity Theft victim, law enforcement or other customer that the University has opened or is maintaining a fraudulent account for a customer engaged in Identity Theft.

V. **Detecting Red Flags**

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the customer opening the account:

1) Require certain identifying information such as name, date of birth, academic records, home address or other identification; and

2) Verify the student’s identity at time of issuance of student identification card (review of driver’s license or other government-issued photo identification).

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

1) Verify the identification of the customer if they request information (in customer, via telephone, via facsimile, via email);

2) Verify the validity of requests to change billing addresses by mail or email and provide the customer a reasonable means of promptly reporting incorrect billing address changes; and

3) Verify changes in banking information given for billing and payment purposes.

C. Protecting Hard Copy

All personnel shall comply with the following requirements:

1) File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with confidential information must be locked when not in use.

2) Storage rooms containing documents with confidential information and record retention areas must be locked at the end of each workday or when unsupervised.

3) Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing confidential information when not in use.

4) Records may only be destroyed in accordance with retention policy and applicable law. Confidential information must be destroyed in a secure manner.

VI. <u>Preventing and Mitigating Identity Theft</u>

In the event University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate

1) Continue to monitor a Covered Account for evidence of Identity Theft;

2) Change any passwords or other security devices that permit access to Covered Accounts;

3) Notify the Red Flag Coordinator for determination of the appropriate step(s) to take;

4) The Red Flag Coordinator may determine the need to provide the customer with a new identification number.

5) The Red Flag Coordinator may notify law enforcement; and

6) Determine that no response is warranted under the particular circumstances.

B. Protect Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University will take the following steps with respect to its internal operating procedures to protect identifying information:

1) Ensure that its website is secure or provide clear notice that the website is not secure;

2) Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information;

3) Ensure that office computers with access to Covered Account information are password protected;

4) Avoid use of social security numbers;

5) Ensure computer virus protection is up to date; and

6) Require and keep only the kinds of account information that are necessary for University purposes.

C. Procedures

If an apparent victim of identity theft makes an appropriate request for information, the Red Flag Coordinator shall supply the account or loan application and the business transaction records to the apparent victim. An appropriate request must be in writing:

Complete the Red Flag Incident Report Form and email or mail it to the Red Flag Coordinator at:

Email: George.Bass@smsu.edu
Mail: Southwest Minnesota State University
Office of Business Services, IL 139
1501 State Street
Marshall, MN 56258

Before supplying the information to the victim, the Red Flag Coordinator must require the victim to provide:

1) Proof of positive identification; and

2) Proof of claim of identity theft

Positive proof of identification is obtained using the current procedure. Proof of an identity theft claim includes:

1) A copy of a police report evidencing the claim of the victim of identity theft; and

2) A properly completed copy of a FTC affidavit of identity theft.

VII. Program Administration

A. Oversight

Responsibility for developing, implementing and updating the Program lies with the Red Flag Coordinator. The Red Flag Coordinator will be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Red Flag Coordinator in the detection of Red Flags and the responsible steps to be taken when a Red Flag is detected.

Annually, University staff will be required to review a Red Flag Power Point and take the Red Flag Training Quiz as prepared by the Minnesota State System Office. The last page of the quiz must be signed and presented to the Red Flag Coordinator.

C. Program Updates

The Red Flag Coordinator will at least annually review and update the program to reflect changes in risks to students and employees and the soundness of the University from Identity Theft. In doing so, the Coordinator will consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Red Flag Coordinator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Red Flag Coordinator shall update the Program.

D. Oversight of Service Provider Arrangements

The University shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedure designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

VIII. **Revision History**

Version: 1.0
Approved: May 13, 2010 by President Danahar