

**Minnesota State University, Mankato**  
**Identity Theft Prevention Program**  
(Updated July 2009)

**BACKGROUND**

**Red Flag Overview, Summary of Law and Regulation:** The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place and must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” –that could indicate identity theft. Unlike many of the other laws and regulations that address data security and data privacy and at least in part look to protect against identity theft, the Red Flags Regulations seek to prevent one who has stolen an identity or is in the process of stealing an identity from being successful in committing a fraudulent act. The regulations look to subject organizations to identify red flags that single out suspicious circumstances and develop processes to protect against possible fraudulent activity when red flags are triggered. The program and efforts under the program are intended to provide additional efforts aimed at detection and prevention of fraudulent activity directed against the University and its students and employees.

On March 18, 2009 the Board of Trustees approved the Minnesota State Colleges and Universities Identity Theft Prevention Program that is expected to be incorporated into a System Guideline under an appropriate Board Policy to provide ongoing accessibility and visibility. On April 2, 2009, Laura M. King, Vice Chancellor/Chief Financial Officer for the Minnesota State Colleges and Universities instructed each college/university to designate an Identity Theft Prevention program administrator to coordinate campus risk assessment, distribute the program as applicable based on risk assessment, develop local guidelines that address risk areas consistent with the program and engage in other program related activities such as training and periodic updating of guidelines. The Identity Theft Prevention program administrator for Minnesota State University, Mankato is Richard J. Straka, Vice President for Finance and Administration.

**PURPOSE**

The purpose of this document is to establish an Identify Theft Prevention Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 designed to detect, prevent and mitigate financial identity theft in connection with the collection of any identifying information throughout Minnesota State University, Mankato.

These guidelines are intended to heighten awareness and:

- Identify patterns, practices, or specific activities (“Red Flags”) that indicate the possible existence of identity theft with regard to new or existing covered accounts;
- Detect Red Flags that have been incorporated into the Program;

- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
- Ensure periodic updating of the Program, including reviewing the accounts that are covered and the identified Red Flags that are part of the Program; and
- Promote compliance with state and federal laws and regulations regarding identity theft protection.

## **DEFINITIONS**

### **Identify theft**

Identity theft means fraud committed or attempted using the identifying information of another person without permission. Financial identity theft occurs when someone uses another consumer's personal information with the intent of conducting transactions to commit fraud that results in substantial harm or inconvenience to the victim.

### **Identifying Information**

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
- d. Social Security or taxpayer identification number
- e. Driver's license or identification number
- f. Alien registration or passport number
- g. Customer number
- h. Date of Birth
- i. Computer's Internet Protocol (IP) address
- j. Banking information and routing number
- k. Credit Card Number
- l. Credit Card Expiration Date

Other items that may be used in conjunction with personal information may be:

- m. Paychecks
- n. Pay stubs
- o. Flexible benefits plan
- p. Doctor names and claims
- q. Insurance claims
- r. Any related personal medical information

### **Red Flag**

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of 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. Alerts, notifications, or warnings from a consumer reporting agency. Examples of these Red Flags include the following:
  - A fraud or active duty alert included with a consumer report;
  - A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
  - A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act; and
  - A consumer report that indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
- b. Suspicious documents. Examples of these Red Flags include the following:
  - Documents provided for identification that appear to have been altered or forged;
  - The photograph or physical description on the identification is not consistent with the appearance of the student, faculty, staff, and other constituent presenting the identification;
  - Other information on the identification is not consistent with information provided by the person opening a new covered account or student, faculty, staff, and other constituent presenting the identification;
  - Other information on the identification is not consistent with readily accessible information that is on file with the University; and
  - An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- c. Suspicious personally identifying information. Examples of these Red Flags include the following:
  - Personally identifying information provided is inconsistent when compared against external information sources used by the University;
  - Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;
  - 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;
  - The SSN provided is the same as that submitted by another student, faculty, staff, or constituent;
  - Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and
  - When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- d. Unusual use of, or suspicious activity related to, the covered account. Examples of these Red Flags include the following:
  - Shortly following the notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account;
  - Payments stop on an otherwise consistently up-to-date account;
  - Account used in a way that is not consistent with prior use;
  - Mail sent to the student is repeatedly returned as undeliverable;
  - Notice to the University that a student is not receiving mail sent by the University;

- Notice that an account has unauthorized activity;
  - Breach in the University's computer system security; and
  - Unauthorized access to or use of client account information.
- e. Alerts from Others--Notice from a client, Identity Theft victim, law enforcement, or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

### **Covered Account**

A covered account is an account that the creditor offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions or any other account that the creditor maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft. Covered accounts include, but are not limited to, credit cards, debit cards, declining balance accounts, loans, and unpaid or partially paid accounts.

### **Creditor**

Creditor means any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. A college or university could be considered a creditor by participating in the Federal Perkins Loan Program, offering institutional loans, maintaining declining balance accounts, or offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

### **IDENTIFICATION OF COVERED ACCOUNTS**

Minnesota State University, Mankato has identified six types of accounts, three of which are covered by the University and three types of accounts administered by service providers.

- a. Refund of credit balances
- b. Short-term loans
- c. MavCASH declining balance accounts
- d. Meal plan/Flex plan dining accounts administered by Sodexo (service-provider)
- e. Federal Perkins Loans, collection administered by ECSI (service-provider)
- f. Tuition payment plan administered by Nelnet/FACTS (service-provider)

### **ESTABLISHING ACCOUNTHOLDER INFORMATION**

#### **Issuance of Account Number (Tech ID)**

In order to establish an account as an admitted student a number of documents must be received and reviewed by University staff which includes high school transcripts, ACT or other standardized test results, and official transcripts from any post-secondary institutions attended. Once admitted, a student is provided with a university Tech ID number.

In order to establish an account as an employee a number of hiring documents must be completed and reviewed by the Office of Human Resources. Once the required documents have been approved, an employee record is created which results in both a State Employee ID number and a university Tech ID number.

Campus network logon access is restricted to currently enrolled students and employees with active or emeriti status. University Information Technology Services conducts routine updates to ensure this restricted access.

### Student Enrollment/Registration

Student course registration is processed via the Minnesota State Colleges and Universities (MnSCU) e-Services web client that requires entry of Student Tech ID and PIN. A number of registration edits control the ability of individual students to update the various enrollment transactions that affect student account charges, based on student records data and timing of financial obligation dates.

### Issuance of University Identification Card

Before issuing a University Identification Card (MavCARD), the student or employee must complete and sign an application and present government-issued photo identification (drivers' license, passport, state-issued ID card, etc.). The application includes the person's name and Tech ID number. The identification card system does not allow the card office employee to create a MavCARD without system-verified credentials, nor does it allow manual changes to the key identifiers such as Tech ID, name, account status (employee or student), or barcode number. The student's or employee's photo is taken and the image is stored in the ID credentials system. The MavCARD is printed on-site and, except for limited pre-defined situations, immediately hand-delivered to the accountholder. MavCARDS for accountholders at off-site locations are entrusted to a specified University employee to hand-deliver each card to the appropriate accountholder.

## PROTECTING ACCOUNTHOLDER INFORMATION

### Receiving Telephone Calls

Before giving information to a caller, the University employee should verify whom they are talking to by asking for the caller's name and Student Tech ID number. As appropriate, the University employee should pursue the inquiry further by requesting the caller to provide other verifiable information such as local or permanent address, date of birth, class registration details and/or other student records information to the degree necessary to provide assurance of the caller's identity.

If the caller is anyone other than the person identified on the account, the University employee should not give information without confirming the required written consent from the student has been provided. Confirming the identity of a third party who has been granted authorization over the phone may require similar requests to verify information such as name, mailing address, relationship to student and/or other student records information to the degree necessary to provide assurance of the caller's identity.

- **Pretext Calling:** Pretext calling is a fraudulent means of obtaining an individual's personal information. Armed with limited information, such as a customer's name, address and/or social security number, a pretext caller may pose as a customer or an

employee in an attempt to convince another employee to divulge confidential information.

- One way that wrongdoers improperly obtain personal information of customers in order to commit identity theft is by contacting someone, posing as a customer or someone authorized to have the customer's information, and convincing an employee to release customer identifying information. It is important that each employee understand this and know what to do if they think it is happening.
- The list below identifies potential pretext caller situations. While calls that resemble these examples are not necessarily pretext calls, extra care should be taken to ensure the authenticity of the call:
  - a. A caller who cannot provide all relevant information;
  - b. An employee caller whose Caller ID does not agree with that employee's location;
  - c. A caller who is abusive and attempts to get information through intimidation;
  - d. A caller who tries to distract a University employee by being overly friendly or engaging the employee in unrelated "chit-chat" in an effort to change the employee's focus and,
  - e. Any caller who appears to be trying to get the employee to circumvent University policy through some tactic that is intended to persuade the employee.

Pretext callers may "nibble" employees until they build a complete customer profile. Callers may also nibble for information about University employees.

After numerous successful attempts the pretext caller has obtained sufficient information to create a complete profile. As such, University employees need to treat all information as highly sensitive and confidential.

It is important to document and detail any unusual telephone calls that you may receive.

### **Face-to-Face Transactions/Inquiries**

Before giving account information, documents that contain an accountholder's personal information, or checks made payable to an accountholder, the University employee should verify whom they are talking to by asking the person to provide his/her name and present his/her University photo ID card (MavCARD) or other government-issued photo identification and Tech ID number.

If the person requesting information is anyone other than the person identified on the account, we should not give information without confirming the required written consent from the student has been provided. Confirming the identity of a third party who has been granted authorization should be done by asking the person to provide his/her name and present his/her government-issued photo identification.

### **E-Mail Inquiries**

Before giving information, the University employee should verify the identity of the person with whom s/he is communicating by requesting the person provide his/her Tech ID number and

confirming the e-mail is sent from an account documented on the Integrated Statewide Records System (Personal or Institutionally managed). Replies to e-mail inquiries should be sent to one or both of the e-mail accounts listed on ISRS.

If the inquiry is from anyone other than the person identified on the account, we should not give information without confirming the required written consent from the student has been provided. Confirming the identity of a third party who has been granted authorization over e-mail may require requests to verify information such as name, mailing address, relationship to student and/or other student records information to the degree necessary to provide assurance of the sender's identity. Replies to e-mail inquiries from third parties should also be sent to one or both of the e-mail accounts listed on ISRS.

### **Change of Address**

Student address updates are processed via the Minnesota State Colleges and Universities (MnSCU) e-Services web client that requires entry of Student Tech ID and PIN.

Employee address updates are processed via the State of Minnesota Employee Self Service site that requires entry of Employee ID and PIN.

### **Change of Name**

Before a name change request is processed, the client is required to provide official documentation such as a copy of the driver's license, marriage certificate or divorce papers, or legal documents changing their name along with a written request to do this.

### **Change of Social Security Number or Taxpayer ID number**

Before an update/correction to a social security or taxpayer ID number is processed, the client is required to provide official documentation (copy of the new social security card or verification of taxpayer ID number change) along with a written request to do this.

### **Change of Direct Deposit Authorization**

A student direct deposit authorization form, containing the student's signature as well as a voided check (checking account) or deposit slip (savings account) attached, is required for a change to be processed. The voided check/deposit slip must also indicate that the name on the bank account matches the name of the student on the student records system.

The University anticipates the change to student direct deposit authorizations to an online process via the Minnesota State Colleges and Universities (MnSCU) e-Services web client that requires entry of Student Tech ID and PIN. This process is currently in development at MnSCU. Employee direct deposit authorization updates are processed via the State of Minnesota Employee Self Service site that requires entry of Employee ID and PIN.

### **Replacement of University Identification Card**

Each cardholder is only allowed once ID card at any time. A cardholder can deactivate his/her card online through a secure web site that requires campus network logon access. A card is also deactivated automatically if a new card is printed for the cardholder. If a card is lost and then found, it can only be reactivated if a replacement card has not been issued and only by card office management once the identity of the person in possession of the card has been verified as the cardholder.

### Protecting Electronically Displayed Data

All personnel shall adhere to safeguarding practices by restricting the ability of others to view private information displayed on computer monitors by logging out or locking out of his/her user account when unattended and/or removing the information from the screen display to prevent visibility by those without authorization to access the information.

### Protecting Hard Copy Material

All personnel shall comply with the following requirements:

- a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Confidential Information must be locked when not in use.
- b. Storage rooms containing documents with Confidential Information and record retention areas must be locked at the end of each workday or when unsupervised.
- c. 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 or in view of those without authorization to access the information.
- d. Records may only be destroyed in accordance with retention policy and applicable law. Confidential information must be destroyed in a secure manner.

### Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more covered accounts, University must take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

1. Require, by contract, that the service provider has such policies and procedures in place; and
2. Require, by contract, that the service provider review the System's Program and report any Red Flags to the responsible Program Administrator or University employee with primary oversight of the service provider relationship.

To comply with these requirements it is recommend that current contracts will be reviewed to determine if they may concern University covered accounts and, if appropriate, an amendment to the appropriate vendor containing the following provision will be proposed:

**RED FLAG RULES.** Vendor agrees that in fulfilling the duties of this agreement, Vendor is responsible for complying with the Federal Trade Commission's Red Flag Rules, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Vendor agrees to have policies and procedures to detect relevant Red Flags that may arise in the performance of this agreement and to take appropriate steps to prevent or mitigate identify theft relating to this agreement. Vendor shall provide a copy of its written program to Minnesota State University, Mankato ("the University"). If requested by the University, Vendor shall report any Red Flags concerning the University's covered accounts and this contract to the University's authorized representative

### PREVENTING AND MITIGATING IDENTITY THEFT

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. Continue to monitor a covered account for evidence of identity theft;
- b. Contact the client;
- c. Change any passwords or other security devices that permit access to covered accounts;
- d. Not open a new covered account;
- e. Provide the client with a new client identification number;
- f. Notify the Program Administrator for determination of the appropriate step(s) to take;
- g. Notify law enforcement;
- h. File or assist in filing a Suspicious Activities Report (“SAR”); or
- i. Determine that no response is warranted under the particular circumstances.

### **WRITTEN NOTIFICATION: IDENTITY THEFT**

The accountholder is required to notify Minnesota State University, Mankato in writing if they suspect they are a victim of identity theft. The initial notification may be made by phone or in writing. The account will be marked but, the client must complete the “Notification of Suspected Identity Theft” form (attached). If a University employee receives such information directly from a working partner, the employee should take information given by the “victim” (i.e., the information must come directly from the client).

Do not give any information regarding the account to the client. It is critical that we first verify we are dealing with the victim of identity theft rather than the perpetrator of the crime. Inform the client that we will contact them after verifying the Police Case Number or FTC affidavit of identity theft form and attached records for five (5) years after the date of receipt. The University should keep a copy of these records also.

### **PROCEDURES, CLIENT REQUEST FOR INFORMATION**

If an apparent victim of identity theft makes an appropriate request for information, the Compliance Officer shall supply the account and the business transaction records to the apparent victim. An appropriate request must:

- a. Be in writing;
- b. Be mailed to:  
University Data Practices Compliance Officer  
Office of the President  
Minnesota State University, Mankato  
309 Wigley Administration Center  
Mankato, MN 56001

Before supplying the information to the victim, the Compliance Officer must require the victim to provide the following:

- c. Positive proof of identification using one or more **current, valid photo identification** including:
  - U.S. driver’s license
  - State issued identification card
  - Passport
  - Military identification card

- d. Proof of claim of identity theft **including both:**
- A copy of a police report evidencing the claim of the victim of identity theft; and
  - A properly completed copy of a FTC affidavit of identity theft

The Compliance Officer will complete the Request of Information Related to Identity Theft and submit the form to the Program Administrator for approval to block the reporting of identity theft information to Credit Reporting Agency. The Program Administrator shall maintain the Request Form and attached records for five (5) years after the date of receipt.

### **ASSISTING VICTIMS OF IDENTITY THEFT**

- a. Suggest that the customer contact the fraud department of each of the three major credit bureaus and request that the credit bureaus place a “fraud alert” and a “victim’s” statement in the customer’s credit file. The fraud alert puts creditors on notice that the customer has been the victim of fraud and the victim’s statement asks creditors not to open additional accounts without first contacting the customer. The following are the phone numbers of the three national credit bureaus:
- Equifax (800)-525-6285
  - Experian (888)-397-3742
  - Trans Union (800)-680-7289
- b. Suggest the customer request from the credit bureaus a free credit report. Credit bureaus must provide a free credit report if the customer believes the report is inaccurate due to fraud.
- c. Suggest the customer contact all financial institutions and creditors where the customer has accounts. The customer should request that they restrict access to the customer’s account, change any password or close the account altogether, if there is evidence that the account has been the target of identity theft.
- d. Suggest the customer file a police report to document the crime;
- e. Suggest the customer contact the Federal Trade Commission (FTC) Identity Theft Hotline at (877) ID-THEFT (438-4338). The FTC puts the information into a secure consumer fraud database and shares it with local, state and federal law enforcement agencies. You may also refer the customer to the following website: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) these resources can provide the customer with step-by-step assistance in handling identity theft.

### **ANNUAL PROGRAM REVIEW**

The Program Administrator will convene a review committee composed of representatives from the Finance and Administration, Academic & Student Affairs, and Information & Technology Services Divisions, on an annual basis. The committee’s charge will be to review and update the Program, which will include reviewing the accounts that are covered and the identified Red Flags that are part of the Program. The committee members will be named and scheduled to meet in April, 2010, for this purpose.

## Request of Information Related to Identity Theft

### NOTIFICATION OF SUSPECTED IDENTITY THEFT

*To be completed by the alleged victim:*

PLEASE PRINT		
Date:        /        /		
1. Full Legal Name: First	Middle	Last
2. Name on Account(s) if different than above:		
3. SSN:	4. Telephone Number (    )	
5. Physical Address:	6. Mailing Address:	
7. Account Number(s) of suspected fraud:		
8. <b>If applicable</b> , please provide account information for all valid accounts with the bank:		
Account#:	Account Type:	
Account#:	Account Type:	

NOTE: you must provide the Police Case Number assigned to this case. The bank will not begin an investigation without a valid case number.

9. **Police Case or FTC affidavit#** \_\_\_\_\_

10. Please provide a detailed statement describing the questioned activity and the documentation that is being requested (attach additional pages if needed):
11. Date of the application or transaction in question:
12. Please list any additional information you may have that will assist with our investigation.
13. I authorize the bank to provide information relating to this case to: (check those that apply): <input type="checkbox"/> Only those that have signed below. <input type="checkbox"/> The following Federal, State, or local government law enforcement agency or officer:

14. By signing below, I _____, attest to the accuracy and truthfulness of the information provided above.		
Signature	Date	<b>NOTARY:</b>