

Table of Contents

BACKGROUND:	2
PURPOSE:	2
DEFINITIONS:	2
GUIDELINES:	3
1. Identify theft	3
2. Changing Account Data.....	3
3. Pretext Calling:	4
4. Receiving Telephone Calls:	5
5. Receiving E-mail:	5
6. In Person:	6
7. Protecting Hard Copy Material.....	6
8. Red Flags	7
9. Preventing and Mitigating Identity Theft:	8
10. Written Notification: Identity Theft:	8
11. Requests for Information from Victims of Identity Theft:	9
12. Assisting Victims of Identity Theft:	9
13. Service Provider Arrangements:.....	10
14. Links	11
NOTIFICATION OF SUSPECTED IDENTITY THEFT	12
AMENDMENT TO AGREEMENT.....	13

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.

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 identity theft in collection of any identifying information throughout St. Cloud State University.

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:

Wherever and whenever the following words or their pronouns occur in this proposal, they shall have the meaning given here:

- Customer: any person for which we maintain detailed, personal data. May include, but is not limited to: students (past, present or prospective), employees (both past and present) or community members.

St. Cloud State University—Identity Theft Prevention Program
Effective November 1, 2009

Directory or Public information:

a. Student:

Directory (public) information includes:

- Personal - name, address (local and permanent), phone number, e-mail address, hometown,
- Academic - graduation date, major, status (full/part time), degrees, honors and awards received, dates of attendance, participation in officially recognized activities and sports, athletic height and weight, and photo (stills or motion).

b. Employee:

The listing of public data includes: name, gross salary, salary range, job title, education and training, dates of employment, work location, office telephone, city and county of residence, value and nature of fringe benefits, expense reimbursement, job description, previous work experience, existence and status of any complaints or charges against the employee, final disposition of disciplinary action, honors and awards received, timesheets, employee ID (not SSN). All other information on employees is private.

- Personal or confidential information: all customer information not specifically designated as directory or public information, whether stored in electronic or printed format.

GUIDELINES:

1. 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.

2. Changing Account Data

If a customer asks you to change their name:

Request they send official documentation such as a copy of the driver's license, marriage certificate or divorce papers, social security card or legal documents changing their name along with a written request to do this. This request is consistent with MnSCU Guidelines for Maintaining Core Data.

If a customer requests you change their social security or taxpayer ID number:

Request they send official documentation (copy of the new social security card or verification of taxpayer ID number change) along with a written request to do this. Again, this request is consistent with MnSCU Guidelines for Maintaining Core Data.

If a customer requests to change their address:

The SCSU staff person should verify whom they are talking to by asking their full name and school tech ID or SSN, and to verify one or more of the following: address, date of birth, email address or phone number.

If after verifying data, the SCSU employee is not confident of the person's identity, the employee should continue to ask questions or refer the caller to their supervisor.

If the requestor is anyone other than the person identified on the account, we should not change information without a signed Release of Information form on file from the customer.

Once the information is verified, the address may be changed.

3. 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 student or an employee in an attempt to convince a SCSU staff person 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 a SCSU staff person to release customer identifying information. It is important that each staff person 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 SCSU staff person by being overly friendly or engaging the staff person in unrelated "chit-chat" in an effort to change the staff person's focus and,
 - e. Any caller who appears to be trying to get the staff person to circumvent SCSU policy through some tactic that is intended to persuade the staff person.

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

After numerous successful attempts the pretext caller has obtained sufficient information to create a complete profile. As such, SCSU 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. Staff persons who receive unusual or suspicious telephone calls should report them to their supervisor who will log the telephone call information and share it with other supervisors and/or staff as necessary. Supervisors will monitor and provide information to staff if it appears that there is a pattern of calls that seem suspicious.

4. Receiving Telephone Calls:

Before giving personal information to a caller, the SCSU staff person should verify who they are talking to by asking the caller their full name and school tech ID or SSN, and to verify one or more of the following: address, date of birth, email address or phone number: full name, school tech ID, address, date of birth, email address or phone number.

If after verifying data, the SCSU employee is not confident of the person's identity, the employee should continue to ask questions or refer the caller to their supervisor.

If the caller is anyone other than the person identified on the account, we should not provide information without a signed Release of Information form on file from the customer.

Caution: Be very careful when talking to anyone other than the person on the account. If they seem to be fumbling, or fishing for information from you- **be aware!**

5. Receiving E-mail:

Before giving personal information via e-mail, the SCSU staff person should verify whom they are communicating with by asking their full name and school tech ID or SSN, and to verify one or more of the following: address, date of birth, email address or phone number: full name, school tech ID, address, date of birth, email address or phone number. Thus, if the initial e-mail does not include enough identifying data, send a return e-mail requesting the needed data.

If after verifying data, the SCSU employee is not confident of the person's identity, the employee should continue to ask questions or refer the person to their supervisor.

If the sender is anyone other than the person identified on the account, we should not provide information without a signed Release of Information form on file from the customer.

6. In Person:

To help protect private data when talking in person with a customer the SCSU staff person should:

1. Have the student input their SSN or ID number into a wireless keypad.
2. Request to see a picture ID.

If a picture ID is not available, the SCSU employee should ask the customer to verify their full name and one or more of the following: address, date of birth, email address or phone number.

If after verifying data, the SCSU employee is not confident of the person's identity, the employee should continue to ask questions or refer the person to their supervisor.

If the person is anyone other than the person identified on the account, we should not provide information without a signed Release of Information form on file from the customer.

Clear all screens when finished working with a customer so no private data is available for viewing by unauthorized individuals.

7. Protecting Hard Copy Material

All hard copy material should be secured in one or more of the following ways:

- a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Confidential Information must be locked when not in use or when the office space/work area is not locked or secure.
- 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 when the office space/work area is not locked or secure.
- d. Records may only be destroyed in accordance with retention policy and applicable law. Confidential information must be destroyed in a secure manner.

8. Red Flags

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 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
- d. Unusual use of, or suspicious activity related to, the covered account. Examples of these Red Flags include the following:

St. Cloud State University—Identity Theft Prevention Program
Effective November 1, 2009

- 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 customer account information.
- e. Alerts from Others--Notice from a customer, 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.

9. 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 the Account for evidence of Identity Theft;
- b. Contact the customer;
- c. Change any passwords or other security devices that permit access to Accounts;
- d. Not open a new Account;
- e. Provide the customer with a new customer identification number;
- f. Notify the Program Administrator for determination of the appropriate step(s) to take;
- g. Notify law enforcement;
- h. Determine that no response is warranted under the particular circumstances.

10. Written Notification: Identity Theft:

The customer is required to notify St. Cloud State University 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 customer must complete the "Notification of Suspected Identity Theft" form (attached). If a SCSU staff person receives such information directly from an outside agency the staff person should take information given by the "victim" (i.e., the information must come directly from the customer).

Do not give any information regarding the account to the customer. 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 customer that we will contact them after verifying the Police Case Number or FTC affidavit of identity theft.

11. Requests for Information from Victims of Identity Theft:

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

- a. Be in writing:
- b. Be mailed to:
Kristi Tornquist
Dean of Learning Resources & Technology Services
112 Miller Center
720 Fourth Avenue South
St. Cloud State University
St. Cloud, MN 56301

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

12. 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.

St. Cloud State University—Identity Theft Prevention Program
Effective November 1, 2009

- 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 these resources can provide the customer with step-by-step assistance in handling identity theft.

13. Service Provider Arrangements:

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the 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.

- a. Require, by contract, that the service provider has such policies and procedures in place; and
- b. Require, by contract, that the service provider review the SCSU Program and report any Red Flags to the program Compliance Officer of the University or staff person with primary oversight of the service provider relationship.

To comply with these requirements, review current contracts that may concern SCSU covered accounts and, if appropriate, propose an amendment containing the following provision:

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 SCSU. If requested by SCSU, Vendor shall report any Red Flags concerning SCSU's covered accounts and this contract to SCSU's authorized representative.

Attachment 1 to this guideline document contains a sample amendment containing this language. Authorized representatives for these contracts should also obtain a copy of the vendor's written program.

Finally, the provision should be included in new contracts with vendors implicating SCSU's covered accounts.

14. Links

Federal Trade Commission: Fighting Fraud with the Red Flag Rules – A How-To Guide for Business

<http://www.ftc.gov/redflagsrule>

Federal Trade Commission Federal Register 11/9/2007

<http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf>

Federal Trade Commission Press Release 10/31/2007

<http://ftc.gov/opa/2007/10/redflag.shtm>

Information for Financial Aid Professionals Press Release 10/14/2008

<http://www.ifap.ed.gov/eannouncements/1014FTCRedFlagRules.html>

STATE OF MINNESOTA
MINNESOTA STATE COLLEGES & UNIVERSITIES

RED FLAG RULES

AMENDMENT TO AGREEMENT

WHEREAS, the State of Minnesota acting through its Board of Trustees of Minnesota State Colleges & Universities, acting on behalf of St. Cloud State University (“SCSU”) and _____ (“Vendor”) entered into an Agreement dated _____ establishing their relationship; and

WHEREAS, the Federal Trade Commission promulgated identify theft prevention rules commonly referred to as the Red Flag Rules, which may impact the Agreement between SCSU and Vendor;

WHEREAS, the SCSU and Vendor have agreed that an amendment to their agreement is appropriate;

NOW THEREFORE, the Parties agree to amend the Agreement by adding the following provision to their Agreement:

1. **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 SCSU. If requested by SCSU, Vendor shall report any Red Flags concerning SCSU’s covered accounts and this contract to SCSU’s authorized representative.

Except as herein amended, the provisions of the Agreement remain in full force and effect.

Minnesota State Colleges and Universities
St. Cloud State University Guidelines—Identity Theft Prevention Program
Sample Service Provider Contract Amendment

Attachment 1

IN WITNESS WHEREOF, the parties have caused this Amendment to be duly executed intending to be bound thereby.

APPROVED St. Cloud State University: **A MnSCU University**

By (authorized system office signature)
Title
Date

2. _____, **Vendor:**

By (authorized signature)
Title
Date