# RED FLAGS IDENTITY THEFT GUIDELINES

## 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 Minnesota State 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 Minnesota State Guidelines for Maintaining Core Data.

**If a customer requests to change their address:**
The SMSU 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 SMSU 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.

## 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 SMSU 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 SMSU 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 SMSU 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 SMSU 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 SMSU staff.

After numerous successful attempts the pretext caller has obtained sufficient information to create a complete profile. As such, SMSU 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.

**Receiving Telephone Calls:**

Before giving personal information to a caller, the SMSU staff person should verify who they are and 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 SMSU 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**!

**Receiving Email:**

Before giving personal information via email, the SMSU 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 email does not include enough identifying data, send a return email requesting the needed data.

If after verifying data, the SMSU 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.

**In Person:**

To help protect private data when talking in person with a customer the SMSU 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 SMSU 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 SMSU 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.

04/20/2011