



IDENTITY THEFT PREVENTION PROGRAM

Implemented October 2009

Table of Contents

Background.....	3
Purpose.....	3
Definitions.....	3
Pretext Calling	4
Receiving Telephone Calls	5
Change of Address	5
Protecting Hard Copy Material.....	6
Protecting Information in Electronic Format.....	6
Releasing Student Information	6
Releasing Employee Information.....	6
Overall Security	7
Red Flag Indicators	7
Preventing and Mitigating Identity Theft	8
Written Notification: Identity Theft.....	9
Procedures, Request for Information	9
Assisting Victims of Identity Theft.....	10
Service Provider Arrangements	10
Program Oversight	11
Updating the Program	11
Links	12

Background

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. Riverland Community College (hereinafter “College”) has developed this program (hereinafter “Program”) pursuant to those rules.

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 connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. These guidelines are intended to heighten awareness and:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flag that has been detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the creditor from identity theft.

The Program shall incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

Identity Theft means fraud committed or attempted using the identifying information of another person without authority.

A Covered Account means an account the College offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions or an account that the College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College from identity theft.

A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Program Administrator is the individual designated with primary responsibility for the Program at the College.

Identifying Information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:

- Name (including maiden and/or former name)
- Address
- Telephone number
- Social security number or taxpayer identification number
- Driver's license or identification number
- Alien registration or passport number
- Customer number
- Employee identification number
- Computer's Internet Protocol (IP) address
- Credit card number and expiration date, including cardholder name and address
- Student loan information
- Income tax documents
- Deferred tuition payments
- Bank account and routing numbers

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

- Paychecks
- Pay stubs
- Flexible benefits plan
- Doctor names and claims
- Insurance claims
- Any related personal medical information

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 College 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 MnSCU or College 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 College employees.

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

Receiving Telephone Calls

Before giving information to a caller, the College employee should verify to whom they are talking by saying: “Due to security requirements please verify your name, your tech ID, address, date of birth, and email or phone number. If the caller is anyone other than the person identified on the account, we should not give information without a written consent from the client.”

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!**

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, or legal documents changing their name along with a written request to do this.

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.

Change of Address

If a client calls to change their address, the College employee should verify whom they are talking to by saying: “Due to security requirements please verify your name, your tech ID, address, date of birth, and email or phone number. If the caller is anyone other than the person identified on the account, we should not give information without a written consent from the client.”

Once the information is verified, the address may be changed. For student loans, the Student Loan Servicer, ECSI, will be sending an email to the student: You recently changed your address and if this was not you, please contact us immediately. For non-

student loan accounts, if applicable, the College employee completing the name change will send a verification letter to the client stating the change of address and requesting they contact us if this action was not appropriate.

Protecting Hard Copy Material

All employees shall comply with the following requirements:

- a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Identifying Information must be locked when not in use.
- b. Storage rooms containing documents with Identifying 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 Identifying Information when not in use.
- d. Records may only be destroyed in accordance with retention policy and applicable law. Identifying Information must be destroyed in a secure manner.

Protecting Information in Electronic Format

All employees will comply with the following requirements:

- a. Identifying Information shall not be stored on unsecured or unprotected desktop or laptop computers.
- b. Sensitive information shall not be stored on home computers, personal mobile devices, or portable media.
- c. Securely store and distribute all sensitive information in an electronic format.
- d. Never send Identifying Information by email.
- e. Credit card information should only be stored in compliance with Payment Card Industry Data Security Standards (PCIDSS).

Releasing Student Information

A parent may obtain information involving an adult son or daughter with a signed FERPA release form submitted by the student. Employees who have access to data must understand and comply with the FERPA regulations that state “information is not provided unless approved in writing”. Students are required to give this written authorization to the Registrar’s Office if their information is to be shared with another party.

Releasing Employee Information

The College is sensitive to the personal data that is maintained in employee personnel files and will not share information except with the written consent of the employee.

Overall Security

Social Security numbers are not used as student or employee identification numbers. Access to non-directory student data in ISRS is restricted based on employees' duties. Employees who have approved access to the administrative information database may only use the information to perform official College duties. Employees with access to non-directory student data must be trained regularly on FERPA and Red Flag regulations.

Red Flag Indicators

The following Red Flags are potential indicators of fraud. Anytime 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
- 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 College; 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 College;
 - Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College;
 - Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College;

- 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 College; 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 College 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;
 - A request to mail something to an address not listed on file;
 - Mail sent to the student is repeatedly returned as undeliverable;
 - Notice to the College that a student is not receiving mail sent by the College;
 - Notice that an account has unauthorized activity;
 - A request made from a non-college issued e-mail account;
 - Breach in the College’s or ECSI’s computer system security; and
 - Unauthorized access to or use of client account information.
- e. Alerts from Others – Notice from a customer, Identity Theft victim, law enforcement, or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Preventing and Mitigating Identity Theft

In the event College 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 customer or employee;
- c. Change any passwords or other security devices that permit access to Covered Accounts;
- d. Not open a new Covered Account;
- e. Provide the customer or employee with a new College 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 customer or employee is required to notify Minnesota State Colleges & Universities 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 or employee must complete the “Notification of Suspected Identity Theft” form (attached). If a College 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 customer or employee).

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

Procedures, Request for Information

If an apparent victim of Identity Theft makes an appropriate request for information, the College Compliance Officer shall supply the account or loan application and the business transaction records to the apparent victim. An appropriate request must:

- a. Be in writing:
- b. Be mailed to:
Riverland Community College
1900 8th Avenue NW
Austin, MN 55912

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. (For student loans this step must be processed by ECSI as they are the servicer of our loans). The Program Administrator shall maintain the Request Form and attached records for five (5) years after the date of receipt. The Compliance Officer should keep a copy of these records as well.

Assisting Victims of Identity Theft

- a. Suggest that the customer or employee 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 or employee 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 or employee contact all financial institutions and creditors where the customer or employee has accounts. The customer or employee should request that they restrict access to the 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 or employee file a police report to document the crime.
- e. Suggest the customer or employee 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 or employee to the following website: www.consumer.gov/idtheft; these resources can provide the customer with step-by-step assistance in handling Identity Theft.

Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College 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 College’s Program and report any Red Flags to the responsible Program Administrator of the College or employee with primary oversight of the service provider relationship.

To comply with these requirements, review current contracts that may concern MnSCU 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 MnSCU. If requested by MnSCU, Vendor shall report any Red Flags concerning MnSCU's covered accounts and this contract to MnSCU'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 MnSCU's covered accounts.

Program Oversight

Responsibility for developing, implementing and updating this Program lies with the College's Vice President of Finance and Facilities. The Vice President is responsible for:

- Program administration;
- Ensuring appropriate training of the College's employees on the Program;
- Reviewing staff reports regarding the detection of red flags on the identified Covered Accounts and the steps for preventing and mitigating identity theft;
- Determining which steps of preventions and mitigation should be taken in particular circumstances; and
- Considering periodic changes to the Program.

Updating the Program

The Program will be periodically reviewed and updated to reflect changes in risks to students and employees.

1. The Program will be re-evaluated annually to determine whether all aspects of the Program are current and applicable in the current business environment.
2. Periodic reviews will include an assessment of which accounts are covered by the Program.
3. As part of the review, Red Flags may be revised, replaced, or eliminated.
4. Revisions involving actions to take in the event that fraudulent activity is discovered may be needed to reduce damage to the College, its employees, and students.

Links

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>