

University of Vermont and State Agricultural College

Board of Trustees

Red Flag Rule Program

Background

The Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act), to be implemented no later than May 1, 2009 that is intended to reduce the risk of identity theft. This program is intended to detect, prevent, and mitigate opportunities for identity theft at the University of Vermont (UVM). The Red Flag Rule applies to UVM due to our participation in the Federal Perkins Loan program, our institutional loan programs, our extension of credit for student accounts, and the fact that we request background checks that may be “credit reports” for some potential employees and for certain students. Our analysis of the type and scope of activity covered in the regulation, and our risk assessment of potential identity theft opportunities has resulted in a determination that there is a low level risk of possible identity theft at the University of Vermont.

Scope of Covered Activities

- Participation in Federal Perkins Loan Program
- Institutional student loan programs
- Payment plans and promissory notes for covered student accounts.
- Background checks/credit reports in employee hiring process and for students enrolled in certain programs

Existing Policies and Practices

Many offices at UVM maintain files, both electronic and paper, of student biographical, academic, health, financial, and admission records. These records may also include student billing information, Federal Perkins Loan records, and personal correspondence with students and parents. Policies to insure compliance with Gramm-Leach-Bliley Act (GLB), Family Educational Rights and Privacy Act (FERPA), system and application security, and internal control procedures provide an environment where identify theft opportunities are mitigated. Records are safeguarded to ensure the privacy and confidentiality of student, parents, alumni and employees.

The Office of Human Resources performs credit and criminal background checks on some potential employees prior to their date of hire. This population includes police services employees. Additionally, criminal background checks are performed during the

admission process for undergraduate and graduate level nursing students and for students applying to the College of Medicine. Many clinical placement sites also require background checks for students during clinical/practical training.

The University's controls over privileged information include:

- Students are given the opportunity to set up an authorized payer that enables a third party (ex. Parents, or grandparents) access to their student account which includes information regarding their bill only.
- Access to non-directory student data in UVM's Banner system is restricted to those employees of the University with a need to properly perform their duties. These employees are trained to know FERPA and Red Flag regulations.
- Social Security numbers are not used as primary student identification numbers and this data is classified as non-directory student data.
- Student Financial Services employees managing covered accounts are trained to know FERPA and Red Flag regulations.
- The University is sensitive to the personal data (unlisted phone numbers, dates of birth, etc.) that it maintains in its personnel files and databases. We will not disclose personal information, except by written request or signed permission of the employee (for example, the Campus Directory), or unless there is a legitimate business "need-to-know", or if compelled by law.
- Every effort is made to limit the access to private information to those employees on campus with a legitimate "need-to-know." University staff members who have approved access to the administrative information databases understand that they are restricted in using the information obtained only in the conduct of their official duties. The inappropriate use of such access and/or use of administrative data may result in disciplinary action up to, and including, dismissal from the University.
- The University's official personnel files for all employees are retained in the Human Resources Office. Employees have the right to review the materials contained in their personnel file.
- The University's College of Nursing and Health Sciences and College of Medicine each have policies and procedures relating to obtaining and safeguarding information obtained through background checks of students.
- The University has policies that address the safeguarding of various forms of confidential information. Those policies include:
 - Code of Business Conduct http://www.uvm.edu/~uvmppg/ppg/general_html/businessconduct.pdf
 - Computer and Network Use <http://www.uvm.edu/~uvmppg/ppg/cit/compose.pdf>
 - FERPA Rights Disclosure <http://www.uvm.edu/~uvmppg/ppg/student/ferpa.pdf>
 - Records Retention http://www.uvm.edu/~uvmppg/ppg/general_html/recordretention.pdf

Detecting Red Flag Activity

The University's risk assessment has identified the following potential "red flags" as pertaining to its business activities:

- Address discrepancies noted in background check reports
- Presentation of suspicious documents
- Photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification

- Personal identifying information provided is not consistent with other personal identifying information on file with the University
- Documents provided for identification that appear to have been altered or forged
- Unusual or suspicious activity related to covered accounts
- Notification from students, borrowers, law enforcement, or service providers of unusual activity related to a covered account
- Notification from a credit bureau of fraudulent activity

Responding to Red Flags

- Should an employee identify a “red flag” (patterns, practices and specific activities that signal possible identity theft as identified above), they are instructed to bring it to the attention of Director of the Student Financial Services, the Director of Human Resources, or University Registrar immediately. The administrator will investigate the threat of identity theft to determine if there has been a breach and will respond appropriately to prevent future identity theft breaches. Additional actions may include notifying and cooperating with appropriate law enforcement, notifying the student or employee of the potential for attempted fraud and notifying background check vendors of any address discrepancies between information contained in the background check report and the University’s records.

Oversight of Service Providers

- UVM employs Educational Computing Services Inc. (ECSI), a loan servicer for the purpose of billing and collection of Federal Perkins and UVM institutional loan payments. The only information that is shared with ECSI is information required to properly bill and collect loan payment as established by the Department of Education. This includes student name, address, telephone number, social security number, and date of birth. UVM will collect and maintain on file documents from ECSI confirming their compliance with “Red Flag Rules”.
- UVM uses several collection agencies for the purpose of collecting overdue student receivables, defaulted Institutional and Federal Perkins Loans. The only information that is shared with the collection agencies is that information required to perform address searches, and to properly bill and collect payment. This includes student name, address, telephone number, social security number, and date of birth. UVM will collect and maintain on file documents from all collection agencies regarding their compliance with “Red Flag Rules”.
- UVM employs Tuition Management Services (TMS), a tuition billing service, for monthly tuition payment plans. The only data that is shared with the TMS is information relating to the tuition payment plan established by the student or parent. UVM provides TMS with the student name, id, University e-mail, phone number, class and address. UVM will collect and maintain on file documents from TMS confirming its compliance with Red Flag Rules.
- UVM uses Nelnet to host our monthly billing statements and process on-line payments for tuition accounts. The only information that is shared with Nelnet is the student name, student id, address, and billing transactions. UVM will collect and maintain on file documents from Nelnet regarding their compliance with Red Flag Rules.
- UVM uses Pearson Government Solutions to print and host our 1098T. The only information that is shared with Pearson is the student name, social security number, address, and pertinent tax information. UVM will collect and maintain on file documents from Pearson regarding their compliance with Red Flag Rules.
- UVM contracts with Applicant Insight to perform background checks for employees and with Verified Credentials or Certiphi to perform background checks for students. UVM reviews the

vendors' security policies with regard to information in any background check reports to ensure that the vendors adequately safeguard sensitive information.

Periodic Update of Program

This program will be re-evaluated on or about the first day of each calendar year to determine whether all aspects of the program are up to date and applicable in the current business environments, and revised as necessary.

Program Oversight

Operational responsibility of the program is delegated to the Director of Student Financial Services and the University Registrar. The University Official responsible for the oversight and administration of this program is the Vice President for Enrollment Management.

Internal Procedures for Red Flag Rule

I. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the University considers the types of accounts that 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 University identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information;
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student (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 student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person'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

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop 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 student is repeatedly returned as undeliverable;
5. Notice to the University that a student 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 student account information.

E. Alerts from Others

1. Notice to the University from a student, 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.

II. DETECTING RED FLAGS

A. 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:

Detect

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
2. Only accept requests to change billing addresses by mail or University assigned email and provide the student a reasonable means of promptly reporting incorrect billing address changes

B. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment position or application to an academic program or activity for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

II. 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:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student or applicant;
3. Contact the vendor providing a credit report if there is an address discrepancy
4. Change any passwords or other security devices that permit access to Covered Accounts;
5. Provide the student with a new student identification number;
6. Notify the Director of Student Financial Services or Human Resources for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report (“SAR”); or
9. Determine that no response is warranted under the particular circumstances.

Protect Student 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 student identifying information:

1. Ensure that its website is secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student 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 student information that are necessary for University purposes.

IV. PROGRAM ADMINISTRATION

A. Oversight

The Director of Student Financial Services in conjunction with the University Registrar will be responsible for the performance of this program under the oversight of the Vice President for Enrollment Management. These responsible parties will designate a Program Administrator who will be responsible for the operational activities of the program. These operational activities include responsibilities 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, for determining which steps of prevention and mitigation should be taken in particular circumstances, for oversight of service provider compliance and for initiating the annual review of the Program with recommendations for change to be reported to the Vice President for Enrollment Management for consideration and approval.

B. Staff Training and Reports

University staff responsible for implementing the Program shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the

University's failure to comply with this Program. At least annually the Program Administrator shall report to the Director of Student Financial Services and the University Registrar on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

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

D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other University employees or the public. The Program Administrator shall inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Program Updates

The Program Administrator will periodically review and update this Program to reflect changes in risks to students and the soundness of the University from Identity Theft. In doing so, the Program Administrator 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 Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted the Program Administrator will update the Program subject to approval by the Vice President for Enrollment Management.

As approved by the Board of Trustees: May 16, 2009