The University of Vermont

OFFICE OF AUDIT AND COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

Title: Red Flag Rule Program

Policy Statement

The University of Vermont (UVM) participates in the Federal Perkins Loan program, has institutional loan programs, extends credit for student accounts, and requests background checks that may be "credit reports" for some potential employees and for certain students. As such, the University is required to comply with the Federal Trade Commission's (FTC) Red Flag Rule ("the Rule") regulation (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act) which was enacted, in part, to reduce the risk of identity theft. Those covered under the Rule were required to implement a Red Flag Rule Program no later than May 1, 2009.

Reason for the Policy

This Policy documents the University's Red Flag Rule Program ("the Program") which is intended to detect, prevent, and mitigate opportunities for identity theft at the University of Vermont (UVM). While 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, the University commits to implementing the requirements of the Program to mitigate this risk.

Applicability of the Policy

This Policy applies to all University employees with responsibility or control over student records, student billing information, Federal Perkins Loan records, and personal correspondence with students and parents.

Definitions

Covered Account: An account that the University maintains under one of its covered activities.

Covered Activities: Activities that the University participates in which require it to comply with the Red Flags Rule include:

- 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

Red Flags Rule: is a set of regulations that require certain businesses and organizations to develop and implement documented plans to protect consumers from identity theft.

Responsible Administrator: For the purpose of this program, the responsible administrator means the following:

- For student financial data, the Director for Student Financial Services
- For student record data, the Registrar
- For employee data, the Director for Labor Relations and Employment Services

Procedures

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 ensure compliance with Gramm-Leach-Bliley Act (GLBA), 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, parent, alumni, and employee personal and protected information.

The Division of Human Resources, Diversity and Multicultural Affairs (HRDMA) performs credit and criminal background checks on some applicants prior to hire. Additionally, criminal background checks are performed during the admission process for certain students including those applying to undergraduate and graduate level nursing programs and to the Larner College of Medicine. Certain clinical placement sites may also require background checks for students during clinical/practical training.

The University's controls over privileged information include:

- Students are given the opportunity to identify a third-party (i.e., a parent or guardian) to whom the student authorizes access to the billing information contained in their student account.
- Access to non-directory student data in UVM's Banner student information system and the Larner College of Medicine's OASIS system is restricted to those employees of the University with a need to properly perform their duties. These employees are trained to know FERPA, GLBA 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, GLBA and Red Flag regulations.
- The University is sensitive to the personal data (unlisted phone numbers, dates of birth, etc.) that it maintains in its student records and databases. According to FERPA, student record data will not be disclosed, unless an exception applies. Exceptions include:
    - upon receipt of a written request, consent form, or authorization signed by the student to whom the personal information pertains;

- if the personal information is "directory information"
- if the disclosure is to a University official and there is a legitimate business "need-to-know"; or
- if the University is required by law to make the disclosure.

- Every effort is made to limit the access to private information to those employees on campus with a legitimate "need-to-know." University employees who have approved access to the administrative information databases are informed of their responsibilities to safeguard this information and to protect against inappropriate use or disclosure.

- Employees with access understand that they are prohibited from using protected information unless such use is to perform job duties for which they are responsible.

- Employees further understand that the inappropriate access, use or disclosure of personal 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 HRDMA. Employees have the right to review the materials contained in their personnel file.

- Departments that are required to obtain background checks for students have policies and procedures relating to obtaining and safeguarding information obtained through these background checks.

- The University has policies that address the safeguarding of various forms of confidential information. Those policies include, but are not limited to:

  - Code of Conduct and Ethical Standards
  - Computer, Communication, and Network Technology Acceptable Use
  - Gramm-Leach-Bliley Act Information Security Program
  - Information Security Policy
  - Information Security Procedures
  - Privacy
  - FERPA Rights Disclosure
  - Records Management and Retention

Detecting & Responding To Red Flag Activity

Detailed procedures relating to the detection and response to suspected Red Flags can be found in UVM's "Identifying and Responding to Suspected Identity Theft" UOP.

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; and
- Notification from a credit bureau of fraudulent activity.

Should an employee identify a "red flag" (patterns, practices and specific activities that signal possible identity theft as identified above), they are instructed to immediately report this to a Responsible Administrator (refer to the "Definitions" section of this Policy.) In consultation with the Chief Privacy Officer, the responsible 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. The Chief Privacy Officer is responsible to notify the Office of General Counsel and, in the event that electronic data is involved, the Information Security Officer as soon as practicable.

- 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

The University engages in the following activities utilizing third-party service providers:

- UVM employs a third-party loan servicer for the purpose of billing and collection of Federal Perkins and UVM institutional loan payments. The only information that is shared with the loan servicer 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 the loan servicer 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 a third-party tuition billing service for monthly tuition payment plans. The only data that is shared with the tuition billing service is information relating to the tuition payment plan established by the student or payor. UVM provides the tuition billing service with the student name, id, University e-mail, phone number, class and address. UVM will collect and maintain on file documents from the tuition billing service confirming its compliance with Red Flag Rules.

- UVM uses a third-party software to process on-line payments for tuition accounts. The only information that is shared with the third-party host is the student id and balance due. UVM will collect and maintain on file documents from the third-party software provider regarding their compliance with Red Flag Rules.

- UVM uses a third-party to print and host our 1098T. The information that is shared with this third-party host is the student name, social security number, address, transactions, and pertinent tax information. UVM will collect and maintain on file documents from the third-party provider regarding their compliance with Red Flag Rules.

- UVM contracts with third parties to perform background checks for employees and students. UVM reviews the vendors' security policies with regard to information in any background check reports to ensure that the background check contractors 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 revise as necessary. Refer to the Identifying and Responding to Suspected Identity Theft UOP for details.

Program Oversight

The Board of Trustees is responsible for annual review and approval of this Red Flag Rule Program. The Responsible Official listed in the About this Policy section is responsible for this Policy. Day-to-day oversight and implementation responsibilities has been delegated to the Responsible Administrators as defined in this Policy.

These operational activities include:

- ensuring appropriate training of University employees on the Red Flags Rule Program and applicable UOPs;
- reviewing employee reports regarding the detection of Red Flags and/or the suspicion of identity theft;
- ensuring that the appropriate steps are taken to prevent and mitigate identity theft;
- determining which steps of prevention and mitigation should be taken in particular circumstances;
- overseeing service provider compliance; and
- initiating the annual review of the Program with recommendations for change to be reported to the Vice Provost for Enrollment Management for consideration and approval.

Non-disclosure of Specific Practices

For the effectiveness of the Red Flag Rule 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. 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 with the public. Any such disclosures must be pre-approved by the Program Administrator in consultation with the Chief Privacy Officer and/or General Counsel. The Program Administrator is then responsible to inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	**Contact Information:**
Student Financial Services	223 Waterman Building (802) 656-5700 sfs@uvm.edu
Human Resource Services	346 Waterman Building (802) 656-8426 hrs@uvm.edu
Office of the Registrar	360 Waterman Building (802) 656-2045 registrar@uvm.edu
Larner College of Medicine Registrar	Courtyard at Given, Room N 100 (802) 656-0722

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- Code of Business Conduct and Ethical Standards
- Computer, Communication, and Network Technology Acceptable Use
- FERPA Rights Disclosure
- Identifying and Responding to Suspected Identity Theft procedure
- Records Management and Retention

Regulatory References/Citations

- Red Flag Rule (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act)

Training/Education

Training/education related to this policy is as follows:

Training Topic:	Red Flags Rule Training		
Training Audience:	Employees Responsible for Implementing the Program	**Delivered By:**	Student Financial Services
Method of Delivery:	On-Line	**Frequency:**	Prior to providing access to student financial information.

Training Topic:	Detecting Identity Theft		
Training Audience:	Applicable Employees	**Delivered By:**	Student Financial Services
Method of Delivery:	On-Line	**Frequency:**	As Needed/Identified

Other training as identified by the Responsible Official.

About This Policy

Responsible Official:	Vice Provost for Enrollment Management	**Approval Authority:**	Board of Trustees Delegated to President
Policy Number:	V. 2.31.2	**Effective Date:**	May 16, 2009
Revision History:	• March 15, 2021		