OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

UNIVERSITY OPERATING PROCEDURE

FOR PRINTED USE ONLY

Title: Identifying and Responding to Suspected Identity Theft

Overview

This UOP outlines the steps employees must take in the event of identified or suspected identity theft as required under the Red Flags Rule.

Applicability of the Procedure

This Policy applies to all University employees and vendors.

Definitions

Definitions for this UOP are the same as those listed in the Red Flag Rules Program Policy.

Procedures

In its role as a lender and a University that offers credit to students, UVM is required to comply with the Federal Trade Commission's Red Flags Rule. Compliance with this UOP is required for all University activities related to its loan and lending programs; however, the steps outlined herein are considered best practices even for activities that fall outside of those programs. Therefore, employees should refer to this UOP whenever an employee identifies or suspects a case of identity theft.

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

a) Report of fraud accompanying a credit report;

b) Notice or report from a credit agency of a credit freeze on an applicant;

c) Notice or report from a credit agency of an active duty alert for an applicant;

d) Receipt of a notice of address discrepancy in response to a credit report request; and

e) Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

a) Identification document or card that appears to be forged, altered or inauthentic;

b) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

c) Other document with information that is not consistent with existing student information;

d) Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

a) Identifying information presented that is inconsistent with other information the student (example: inconsistent birth dates);

b) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);

c) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

d) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

e) Social security number presented that is the same as one given by another student;

f) An address or phone number presented that is the same as that of another person;

g) A person fails to provide complete personal identifying information on an application when reminded to do so; and

h) 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

a) Change of address for an account followed by a request to change the student's name;

b) Payments stop on an otherwise consistently up-to-date account;

c) Account used in a way that is not consistent with prior use;

d) Mail sent to the student is repeatedly returned as undeliverable;

e) Notice to the University that a student is not receiving mail sent by the University;

f) Notice to the University that an account has unauthorized activity;

g) Breach in the University's computer system security; and

h) Unauthorized access to or use of student account information.

E. Alerts from Others

Notice to the University from a student or employee, a victim of identity theft, 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 employees will take the following steps to monitor transactions on an account:

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, through myUVM self-service portal, 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 employees will take the following steps to assist in identifying address discrepancies:

a) 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
b) 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.

III. Preventing and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags, such personnel shall consult with a manager or supervisor. Managers/supervisors will refer the matter to a Responsible Administrator as defined in UVM's Red Flag Rule Program Policy.

In coordination with the manager, the Responsible Administrator 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 student or applicant;

c) Contact the vendor providing a credit report if there is an address discrepancy;

d) Change any passwords or other security devices that permit access to Covered Accounts;

e) Provide the student with a new student identification number;

f) Notify the Director of Student Financial Services or Chief Human Resource Officer 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.

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 any websites collecting or processing protected information are 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 or devices with access to Covered Account information are password protected;
4. Avoid use of social security numbers;
5. Ensure virus protection is up to date; and
6. Require and keep only the kinds of student information that are necessary for University purposes.

IV. Reporting

University employees are expected to report known or suspected identity theft to the Responsible Administrator in accordance with the Red Flag Rule Program Policy.

At least annually the Program Administrator, as defined in the Red Flag Rules Program Policy shall report to the Director of Student Financial Services, the University Registrar, and the Director for Labor Relations and Employment Services 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.

V. Service Provider Arrangements

For those activities that relate to a covered account, the University will take the following steps to ensure service providers perform their activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. The University will require that service providers providing activities related to covered accounts:

    a) enter into a written contract; and

    b) such contract includes insurance and indemnification clauses.

2. Service providers are also required to:

    a) have such policies and procedures in place;

    b) review the University's Red Flag Rule Program and report any Red Flags to the Program Administrator or to the University employee with primary oversight of the service provider relationship. The University employee with primary oversight of the service provider relationship is subsequently required to report this to the Program Administrator.

VI. Program Updates

In accordance with the University's Red Flag Rule Program Policy, the Program Administrator will periodically review and update the 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 and the Board of Trustees.

Contacts

Questions concerning the daily operational interpretation of this UOP should be directed to the following:	
Title(s)/Department(s):	**Contact Information:**
Student Financial Services	225 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 Admissions	Courtyard at Given, Room N 100 (802) 656-0722

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- Red Flag Rule Policy

Training/Education

Training related to this UOP is outlined in the Red Flag Rules Program Policy.Additional training may be provided on an as-needed basis as determined by the Approval Authority or the Responsible Official.

About This Procedure

Responsible Official:	Vice Provost for Enrollment Management	**Approval Authority:**	Vice Provost for Enrollment Management
Affiliated Policy Number(s):	V. 2.31.1	**Effective Date:**	March 10,2021
Revision History:	None		