

Oregon University System
Identity Theft Prevention Program
Effective May 1, 2009

I. PROGRAM ADOPTION

The Oregon University System ("System") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Oregon University System Board. After consideration of the size and complexity of the System's operations and account systems, and the nature and scope of the System's activities, the Board determined that this Program was appropriate for the System, and therefore approved this Program on April 3, 2009.

II. PURPOSE

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a new covered account or the use of an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts the System 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 flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

III. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

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

A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

A "Covered Account" is an account that the System maintains, primarily for personal, family or household purposes that involves, or is designed to permit multiple payments or transactions.

The "Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VI below.

“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, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the System is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect red flags that have been incorporated into the Program;
Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from identity theft.

The Red Flags Rule allows the System to base its program on the relative risks of identity theft in connection with its covered accounts. Based on the experience of its member institutions, the System considers the risk of identity theft in connection with its covered accounts to be low. Accordingly, this Program has been developed based on that assessment of risk.

IV. COVERED ACCOUNTS

The System has identified 11 types of accounts, 1 of which is covered accounts administered by the System and multiple types of account that are administered by service providers.

System covered accounts:

1. Refund of credit balances involving student loans
2. Deferment of tuition payments
3. Emergency loans
4. Bookstore charges
5. Student Health Center Charges
6. Federal Family Education Loan Program (FFELP) – (Stafford & PLUS)
7. Federal Perkins Loan Program
8. Jesse M. Bell Memorial Loan Fund
9. Revolving Charge Account Plan
10. William D. Ford Federal Direct Loan Program

Service provider covered accounts:

1. "Higher One" Refund Disbursement Program – w/Debit Card (refer to Section VIII (C) for oversight of service provider arrangements).

V. IDENTIFICATION OF RELEVANT RED FLAGS

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts-- acceptance to System campuses and enrollment in classes may require some or all of the following information, subject to campus admission policies and student enrollment status:
 - a. Common application with personally identifying information
 - b. high school transcript
 - c. official ACT or SAT scores
 - d. two letters of recommendation
 - e. Entrance Medical Record
 - f. medical history
 - g. immunization history
 - h. insurance card
3. The methods provided to access covered accounts:
 - a. Disbursement obtained in person require picture identification
 - b. Disbursements obtained by mail can only be mailed to an address on file
4. The System's previous history of identity theft.

The System identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

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

Red Flags

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; and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
3. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
4. Social security number presented that is the same as one given by another student; and
5. A person fails to provide complete personal identifying information on an application when reminded to do so.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

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 System that a student is not receiving mail sent by the System;
6. Notice to the System that an account has unauthorized activity;
7. Breach in the System's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others

Red Flag

1. Notice to the System from a student, identity theft victim, law enforcement, service provider or other source that the System has opened or is maintaining a fraudulent account for a person engaged in identity theft.

VI. DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, System personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification) or follow identification verification processes administered by service providers for covered accounts.

B. Existing Accounts

In order to detect any of the red flags identified above for an existing covered account, System 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. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
3. Confirm changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests

In order to detect any of the red flags identified above for an employment or volunteer position for which a credit report is sought, System personnel will take the following steps to assist in identifying address discrepancies:

1. Require 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 System has reasonably confirmed is accurate.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

In the event System personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of perceived 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 (for which a credit report was run);
3. Change any passwords or other security devices that permit access to covered accounts;
4. Limit the use of SSN to what is absolutely necessary;
5. Notify any service provider with covered account;
6. Not open a new covered account;
7. Provide the student with a new student identification number;
8. Notify the Program Administrator for determination of the appropriate step(s) to take;
9. Notify law enforcement;
10. File or assist in filing a Suspicious Activities Report (“SAR”); or
11. 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 System will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student identity 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. Use encryption and firewall technology;
5. Avoid use of social security numbers (See OUS Information Security Policy);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of student information that are necessary for System purposes.

VIII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) for the System. The Committee is appointed by the Vice Chancellor for Finance and Administration and will be made up of a Chancellor’s Office representative and a Program Administrator from each OUS campus. The Program Administrator at each campus will be responsible for ensuring appropriate training of System staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

System staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. System staff shall be trained, as necessary, to effectively implement the Program. System employees are expected to notify the Program Administrator at their campus once they become aware of an incident of Identity Theft or of the System's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, system staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator 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 System engages a service provider to perform an activity in connection with one or more Covered Accounts, the System 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 System's Program and report any Red Flags to the Program Administrator or the System employee with primary oversight of the service provider relationship.
3. Require, by contract, that service providers formally acknowledge and accept relevant and specifically identified provisions within the System's Program.

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 the Committee and 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 System employees or the public. The Program Administrator at each campus 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 Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the System from Identity Theft. In doing so, the Committee will consider the System's experiences with Identity Theft situations, changes in Identity Theft methods, changes in

Identity Theft detection and prevention methods, and changes in the System's business practices and arrangements with other entities. After considering these factors, the Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.