Program Adoption

Olivet Nazarene University ("University") developed this identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("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 University Administrative Team. After consideration of the size of the College's operations and account systems, and the nature and scope of the College's activities, the Administrative Team determined that this Program was appropriate for Olivet Nazarene University, and therefore approved this Program on April 9, 2009.

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 covered account or 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 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 flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to Students and 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.

Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means:

1. An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.
2. A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Identifying Information means 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 tax identification number, or student identification number.

Covered Accounts

Olivet Nazarene University has identified seven types of accounts, four of which are covered accounts administered by the College and one type of account that is administered by a service provider.

College covered accounts:

1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, without PLUS loans
3. Deferment of tuition payments
4. Campus Debit Card (Tiger Dollar) accounts

Service provider covered account:

1. Tuition payment plan administered by Tuition Management Services (T.M.S.), refer to "Oversight of Service Provider Arrangements" on page 5.
2. Tuition payment plan administered by "Tuition Pay" Plan from Higher One, refer to "Oversight of Service Provider Arrangements" on page 5
3. Repayment of Perkins Loans administered by Affiliated Computer Services (A.C.S.), refer to "Oversight of Service Provider Arrangements" on page 5.
4. Processing of online payments and provision of online Student Account information administered by TouchNet, refer to "Oversight of Service Provider Arrangements" on page 5.

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 the College and enrollment in classes requires all of the following information:
   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. Disbursements obtained in person require picture identification
    b. Disbursements obtained by mail can only be mailed to an address on file unless the requesting person presents picture identification and verbally authorizes the address change.
    c. Disbursements obtained by Olivet email where the requesting party utilizes their own ONU email account and references their student id number.
4. The College's previous history of identity theft.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-College issued e-mail account;
4. A request made by phone that cannot provide accurate, matching account identification (eg. Student identification number or social security number from students only – not second parties).
5. A request to mail something to an address not listed on file unless said request is made in person by an individual presenting proper identification; and
6. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
7. Provides suspicious or inconsistent personal identifying information.
8. Unusual use of or other suspicious activity related to a covered account.

Detection of Red Flags

The Program will detect red flags relevant to each type of covered account as follows:

1. **Refund of a credit balance involving a PLUS loan** – As directed by federal regulation (U.S. Department of Education) these balance are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required. **Red Flag** – none as this is initiated by the College.
2. **Refund of credit balance, no PLUS loan** – requests from current students must be made in person by presenting a picture ID or in writing from the student's college issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the college may be made in person with proper identification or made in writing providing accurate, matching identification information. **Red Flag** – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
3. **Deferment of tuition payment** – Tuition payments are divided into three or four equal installments and require the student's signature on that semester's Student Data Sheet. **Red Flag** – none.

4. **Tiger Dollar Account -** Requests regarding account information or to alter account balances must be made in person by presenting a picture ID or in writing from the student's college issued e-mail account. Phone requests must provide accurate and matching account identification information. **Red Flag -** Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
5. **Tuition payment plan** – Students must contact Tuition Management Systems for undergraduate or Tuition Pay (Higher One) for SGCS, outside service providers, and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.
6. **TouchNet Online Account Information** – Students must contact TouchNet, an outside service provider, and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.

Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the Vice President for Finance. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of College's 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.

Updating the Program

This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the College from identity theft. At least once per year, during the fall semester, the Program Administrator will consider the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the University maintains 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.

Staff Training

College 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.

Oversight of Service Provider Arrangements

The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Currently the College uses Tuition Management Systems (TMS) and Tuition Payment Plan by Higher One to administer Tuition Payment Plans, Affiliated Computer Services (ACS) to administer Perkins Loans, and TouchNet to administer student account online services. The University uses the services of Enterprise Recovery Systems and General Revenue as collection services for delinquent student accounts. Students may contact ACS, TMS, Tuition Pay, Enterprise Recovery Systems, General Revenue Services or TouchNet directly through their websites or by telephone and provide personally identifying information to be matched to the records that the College has provided.

Updated on
June 8, 2015 MKW