Amherst College
IDENTITY THEFT PROGRAM

Summary

Amherst College (the “College”) has developed this identity theft program (the “Program”) pursuant to the Federal Trade Commission’s Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Program was developed with oversight by the Treasurer of the College and approval of the Audit Committee of the Board of Trustees.

Purpose

The Program is 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 established 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 flag that has been detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or 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

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

A Covered Account means (i) 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 or (ii) an account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

College Covered Accounts

The College has identified the following covered accounts:

College administered covered accounts - Students:

1. Plus Loans (Amherst is a direct lender; collection is performed by the U. S. Government)
2. Stafford Loans (Amherst is a direct lender; collection is performed by the U. S. Government)
3. Perkins Loans
4. College Institutional Loans
Amherst College
IDENTITY THEFT PROGRAM

5. Deferred Tuition Payments
6. Emergency Loans
7. Computer Loans
8. One-Card Balances
9. Student Accounts

College administered covered accounts - Employees:

1. Mortgages
2. Computer Loans

Service provider covered accounts:

1. Nelnet Campus Commerce Payment Plan
2. ECSI – Collection of Perkins and Institutional Loans

Risk Assessment

For the student related College administered covered accounts listed above, the existing risk is that a fraudulent request is made for a refund on an overpaid account resulting from a loan and/or direct payment. Since the College is solely responsible for issuing refunds on these accounts, the risk resides at the College level.

There is no perceived risk associated with the employee mortgage and computer loan programs. At no point in the process is there a position where funds are owed to the employee. However, if a case did exist where an employee was owed funds due to an “over-withholding”, the funds would be returned to the employee through the standard payroll process. This process maintains its own control structure to ensure proper payment to employees.

The College will 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. However, the processes transacted by these providers represent funds owed to the College, mitigating the risk of theft to the account holders. Additionally, the College will take steps to review the Red Flag policies and procedures enacted by these providers.

Control Procedures

As noted above, the primary risk associated with the covered accounts relates to refunds on student accounts and loan accounts. The following control procedures mitigate this risk:

All refunds on student accounts (including one-card balances) that are in an overpaid position must be initiated by the student owning the account. The request may be initiated either in person, or in writing from the student’s Amherst College e-mail account. Phone requests will not be honored due to the difficulty in accessing the individual’s identity.
Amherst College
IDENTITY THEFT PROGRAM

Requests made in person must be made at the Student Accounts Department within the Comptroller’s Office during standard operating hours. The student must present his/her valid Amherst College identification.

Checks are paid and mailed to the official name and address within the Datatel System or may be picked up in person. The student must once again provide his/her valid Amherst College identification when receiving the check in person. A student may request a specific payee or address that is different from the system data; however, this must be requested in writing and submitted either in person, with valid Amherst College identification, or directly from the student’s Amherst email account.

Students must make any permanent name or address change in the Registrar’s Office. A change in name requires the appropriate legal document subject to the specific instance, such as a marriage certificate. These changes require the student to visit the Registrar’s Office in person and present his/her valid Amherst College ID. A change in address may be requested either through the student’s College e-mail account or in person. If requested in person, the student must show his/her valid College ID.

A change in name or address for an alumnus with loan balances must be made through the Comptroller’s Office. Each alumnus must provide his/her requests in writing and identify his/her personal loan number for verification.

Red Flags

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag is apparent, it should be investigated.

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 to mail something to an address not listed on file; and
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Response to Red Flags

The program provides appropriate responses to detect 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 or employee;
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.
Amherst College
IDENTITY THEFT PROGRAM

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the College’s Treasurer. The Treasurer is responsible for program administration, ensuring appropriate training of the College’s staff on the Program, reviewing any staff reports regarding the detection of red flags on the identified covered accounts 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 employees and the soundness of the College from identity theft related to the noted covered accounts. At least once per fiscal year, the Treasurer 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 College maintains and changes in the College’s business arrangements with other entities, as they relate to this program. After considering these factors, the Treasurer will determine whether changes to the Program, including the listing of red flags, are warranted. If warranted, the Program will be updated.

Staff Training

College staff responsible for implementing the Program shall be trained either by or under the direction of the Treasurer and/or the Comptroller in the detection of red flags, and the responsive steps to be taken when a Red Flag is detected.