Appalachian State University
Identity Theft Prevention Program Procedures

Program Overview

I. PURPOSE

The purpose of the Program is to:
 Identify, detect and respond to Red Flags;
 Prevent and mitigate Identity Theft; and
 Develop departmental Internal Procedures for compliance with the Rule**.**

II. DEFINITIONS

For purposes of the Program, the following definitions apply:
"Covered Account" includes those offered or maintained by the University:

Accounts that involve or are designed to permit multiple payments or transactions, deferred payment arrangements, or extensions of credit, loans, or deposit accounts which establish a continuing financial relationship with individual consumers;

For which there is a reasonably foreseeable risk of Identity theft to consumers or to the safety and soundness of the University, including financial, operational, compliance, reputational, or litigation risks; or

That utilizes credit checks.

"Identity Theft" is a fraud committed using the Identifying Information of another person, subject to such further definition as the Federal Trade Commission may prescribe, by regulation.

"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 any:

Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

Unique electronic identification number, address, or routing code; or

Access device, including any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.

"Program Administrator" is the Director of Special Project, and is responsible for the oversight, development, implementation, and administration of the Program as outlined in the sections below. The Program Administrator shall consult with the University Controller, General Counsel on implementation and maintenance of the Program.

"Program Contact Person" is the employee designated by a University department to act as a liaison between the department's management and the Program Administrator and to assume responsibility for Program duties as outlined in the sections below.

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

"Service Provider" is an outside entity engaged by the University to perform an activity in connection with one or more Covered Accounts.

III. PROGRAM COMPONENTS

The University's Program consists of the following components:

Identifying Covered Accounts;

Identifying relevant Red Flags for new and existing Covered Accounts and incorporating those Red Flags into the Program;

Detecting Red Flags that have been incorporated into the Program;

Responding appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft;

Training employees regarding the Program;

Reviewing Service Provider agreements for compliance with the Program; and

Ensuring the Program is updated periodically to reflect changes in risks to consumers or to the University from Identity Theft.

The University's policy can be found in the Online Resource Manual in the Administrative Policies: Identity Theft Prevention Program.

IV. Procedures

A. Identifying Covered Accounts

In order to identify Covered Accounts, each University department shall make a risk determination of its financial transactional, credit, or loan accounts considering:

Methods used to open and access the account, especially those that do not require face-to-face contact, such as through the Internet or by telephone;

Whether the account has been the target of Identity Theft attempts in the past;

Technological risks (for example, password protection, use of mobile devices, computer controls such as locking screens, automatic logoffs, and physical security measures for work areas both during the workday and during nights/weekends), and

Other accounts if there is a reasonably foreseeable fraud or Identity Theft risk to consumers or to the University.

Each University department having Covered Accounts shall compile a list of Covered Accounts for which it has oversight and incorporate the list into a written Departmental Red Flags Rule Internal Procedures to be submitted to the Program Administrator.

B. Identifying Red Flags

As set forth in the Policy, Red Flags include but are not limited to:
1. The presentation of suspicious documents;
2. The presentation of suspicious Identifying Information;
3. The unusual use of, or other suspicious activity related to, a Covered Account;
4. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services; and
5. Notices from consumers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with Covered Accounts held by the University.

Each University department having Covered Accounts shall compile a list of Red Flags relevant to its covered transactions and incorporate the list into its Internal Procedures.

Appendix A contains examples of Red Flags provided in the Rule but is not an exhaustive list for the purpose of this Program.

C. Detecting Red Flags

Each University department having Covered Accounts shall endeavor to detect Red Flags by developing internal procedures to obtain, verify, and monitor personal Identifying Information of account holders on file with the University. These procedures shall be set forth in the department's Internal Procedures.

D. Responding to Detected Red Flags

Each University department having Covered Accounts shall endeavor to prevent and mitigate Identity Theft associated with its Covered Accounts by developing internal procedures to appropriately respond to detected Red Flags.

Appropriate responses may include:

- Monitoring accounts;
- Contacting consumers;
- Changing passwords;
- Closing and reopening accounts;
- Refusing to open an account;
- Notifying the University's Department of Public Safety;
- Refusing to collect on or "sell" an account;
- Other responses as determined by the department; or
- Determining that no response is warranted.

These procedures shall be set forth in the department's Internal Procedures. Additionally, employees of departments having Covered Accounts are expected to notify their department's Program Contact Person once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program (see also, Section IV). The departmental Program Contact Person shall in turn report the incident to his/her supervisor and the Program Administrator.

E. Training Employees

Each University department having Covered Accounts shall develop a training program and ensure that appropriate employees receive training regarding this Program and the department's Internal Procedures. Names of employees who initially receive training shall be included in the department's Internal Procedures. Thereafter, names of trained employees shall be submitted by the department's Program Contact Person to the Program Administrator on a continuous basis.

F. Reviewing Service Provider Arrangements

In the event that a University department engages a Service Provider to perform an activity in connection with Covered Accounts, the department will ensure the

Service Provider's compliance with this Program by contractually requiring that Service Providers:

1. Have Identity Theft prevention policies and procedures in place;
2. Review the University's Identity Theft Prevention Program and the department's Internal Procedures; and
3. Report detected Red Flags to the department's Program Contact Person and the Program Administrator.

Each University department having Covered Accounts shall identify such Service Providers.

The department's Program Contact Person shall submit the Service Providers' names and contact information in writing to the Program Administrator on a continuous basis.

G. Updating the Program

Upon request by the Program Administrator, each department having Covered Accounts shall periodically review its Internal Procedures to ensure its effectiveness. Consideration for updating Internal Procedures shall be given to:

1. The department's experiences with Identity Theft;
2. Changes in or new methods of Identity Theft;
3. Changes in or new methods of detecting, mitigating, and preventing Identity Theft;
4. Changes in the types of Covered Accounts offered or maintained by the department; and
5. Changes in the University's business arrangements and Service Provider arrangements.

Written reports of Internal Procedures reviews, including any updates made, shall be submitted by the department's Program Contact Person to the Program Administrator in a timely fashion.

V. DEPARTMENTAL RED FLAGS RULE INTERNAL PROCEDURES

Each department having Covered Accounts shall use the template attached as Appendix B to prepare a Internal Procedures containing:
1. The department name and number,
2. The name of and contact information for the person designated as its Program Contact Person;
3. The name of and contact information for the person responsible for Program training within the department (if different from above);
4. A list and description of Covered Accounts;
5. For each Covered Account:
a. A list and description of relevant Red Flags;
b. Internal procedures to obtain, verify, and monitor Identifying Information on file with the University; and
c. Internal procedures to detect and respond to Red Flags; and
6. The names of employees who have received training regarding this Program and the department's Internal Procedures.

Each Internal Procedures will be submitted to the Program Administrator who will append the Internal Procedures to this Program.

VI. PROGRAM ADMINISTRATION

The Program Administrator in consultation with General Council shall be responsible for the implementation, oversight, and continued development of the Program. The appointed Program
Administrator shall have responsibility for:

Acting as the University's primary contact person for the Program;

Providing general support and guidance to departments with Covered Accounts;

Oversight of Program training;

Prompting and approving Internal Procedures reviews and other Program reports;

Working with departments to help ensure Service Providers' compliance with the Program; and

At least annually, reporting to General Counsel on matters related to the Program, including:
o An evaluation of the effectiveness of the current Program;
o Significant instances of Identity Theft that occurred during the reporting period and actions taken in response;
o Status of ongoing monitoring of Service Provider agreements; and
o Any recommendations for material changes to the Program.

Program Administrator Name: Denise Foutz,
Title: Director of Special Projects
Telephone: 828.262.6119 Email: Foutzdn@appstate.edu

VII. AMENDMENTS & UPDATES
This Program may be amended or updated as needed by the Chancellor.

VIII. EFFECTIVE DATE
This Program is effective upon approval by the Board of Trustees.
The University's Board of Trustees adopted this Program on September 24, 2010