Identity Theft Prevention Plan

Policy 105.5

1 Introduction

1.1 Program Adoption

1.1.1 As a best practice and using as a guide the Federal Trade Commission's Red Flags Rule (16 CFR Part 681, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159) and North Carolina General Statutes, Chapter 75, Article 2A, Appalachian State University (the "University") has developed an Identity Theft Prevention Program (the "Program") described below. This Program was developed with oversight and approval of the Board of Trustees of Appalachian State University (the "Board"). After consideration of the size and complexity of the Universitys operations and account systems, and the nature and scope of the Universitys activities, the Board determined that this Program was appropriate for the University, and approved it on September 24, 2010 (the "Effective Date"). The purpose of this Program is to detect, prevent and mitigate identity theft in connection with any covered account. This Program envisions the implementation of policies and procedures subject to the Chancellor's approval in order to achieve these goals.

2 Scope

2.1 All University personnel whose employment duties require or allow access to identifying information of other employees or students are responsible for implementing this Program.

3 Definitions

3.1 "Covered Account"

any account that constitutes a continuing financial relationship or is designed to permit multiple payments or transactions between the University and a person for a service, such as extension of credit, debit cards, Perkins Loans, Federal Family Education Loan Program (FFELP), institutional loans, accounts covered by the Health Insurance Portability and Accountability Act (HIPAA), deposit accounts, scholarship accounts, student accounts, and tuition payment plans.

any other account that the University offers or maintains for which there is a reasonably foreseeable risk to holders of the account or to the University from identity theft, such as use of consumer reports for employee background checks, credit applications and institutional debit card applications. This may include operations of utilities (e.g., New River Light & Power Company), clinical and research activities, and public service activities.

3.2 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, but not limited to:

1. name
2. address
3. telephone number
4. social security number
5. date of birth
6. government-issued driver's license or identification number
7. alien registration number
8. government passport number
9. employer or taxpayer identification number
10. individual identification number
11. computer's Internet Protocol address
12. bank or other financial account routing code

3.3 Identity Theft

means a fraud committed or attempted using the identifying information of another person without authority [16 CFR 603.2(a)].

3.4 Program Administrator

means the individual designated with primary responsibility for oversight of this Program.

3.5 Red Flag

means a pattern, practice, alert or specific activity that indicates the possible existence of identity theft.

3.6 Service Provider

means a person or entity that provides a service directly to the University.

4 Policy and Procedure Statements

4.1 Identification of Red Flags

4.1.1 In order to identify relevant red flags, the University considers the types of covered accounts it offers or maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with identity theft. Red flags may be detected while implementing existing account opening and servicing procedures (example: individual identification, caller authentication, third party authorization, and address changes).

4.1.2 The University identifies the following as red flags in each of the listed categories:

1. Notifications and warnings from consumer reporting agencies
    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
2. Suspicious documents
    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 individual information; and
    4. Application that appears to have been altered or forged.
3. Suspicious personal identifying information
    1. Identifying information that is inconsistent with other information the individual provides (example: inconsistent birth dates);
    2. Identifying information that is inconsistent with other sources of information (example: an address not matching an address on a loan application);
    3. Identifying information that is the same as information shown on other applications that were found to be fraudulent;
    4. Identifying information that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);
    5. Social security number that is the same as one given by another individual;
    6. An address or phone number that is the same as that of another person;
    7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
    8. A person's identifying information is not consistent with the information that is on file for the individual.
4. Suspicious covered account activity
    1. Change of address for an account followed by a request to change the individual'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 individual is repeatedly returned as undeliverable;
    5. Notice to the University that an individual is not receiving mail sent by the University;

6. Notice to the University that an account has unauthorized activity;
7. Breach in the University's computer system security; and
8. Unauthorized access to or use of individual account information.

5. Alerts from others
    1. Notice to the University from an identity theft victim, law enforcement officer or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft.

4.2 Detection of Red Flags

4.2.1 Student Enrollment

4.2.1.1 In order to detect any of the red flags identified above associated with the enrollment of a student, University personnel shall take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the individual's identity at time of issuance of individual

4.2.1.2 Identification card (example: review of driver's license or other government-issued photo identification).

4.2.2 New Customers or Clients

4.2.2.1 In order to detect any of the red flags identified above associated with service to a new customer or client, University personnel shall take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the individual's identity at time of issuance of individual

4.2.2.2 Identification card (example: review of driver's license or other government-issued photo identification).

4.2.3 Existing Accounts

4.2.3.1 In order to detect any of the red flags identified above for an existing covered account, University personnel shall take the following steps to monitor transactions on an account:

1. Verify the identification of individuals 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 individual a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

4.2.4 Consumer ("Credit") Report Requests

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

1. 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
2. In the event that notice of an address discrepancy is received, verify that the credit or background 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.

4.3 Response to Red Flags

4.3.1 Once potentially fraudulent activity is detected, an employee must act promptly to protect individuals and the University from damages and loss. At a minimum, the employee must gather all related documentation, write a description of the situation, and present this information to the program administrator.

4.3.2 The program administrator will complete additional investigation if necessary to determine whether the attempted transaction was fraudulent or authentic.

4.3.3 If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include (1) canceling the transaction; (2) notifying and cooperating with appropriate law enforcement personnel; (3) determining the extent of liability of the University; and (4) notifying the individual upon whom fraud has been attempted or whose identifying information has been subjected to a security breach.

4.4 Prevention and Mitigation of Identity Theft

In the event University personnel detect any identified red flags, such personnel shall take one or more of the following steps to prevent and mitigate identity theft, depending on their determination of the degree of risk posed by the red flag:

1. Continue to monitor a covered account for evidence of identity theft;
2. Contact the individual or applicant (for whom a credit or background report was run);
3. Change any passwords or other security devices that permit access to covered accounts;
4. Refuse to open a new covered account;
5. Provide the individual with a new individual identification number;
6. Notify the program administrator for determination of the appropriate step(s) to take;
7. Notify appropriate law enforcement personnel;
8. File or assist in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network, United States Department of the Treasury; and/or
9. Determine that no response is warranted under the particular circumstances.

4.4.1 Protect Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the University will take the following steps to protect individual 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 individual account 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. Ensure that laptops are password protected and encrypted;
5. Avoid use of social security numbers;
6. Ensure the security of the physical facility that contains covered account information;
7. Ensure that transmission of information is limited and encrypted when necessary;
8. Ensure computer virus protection is up to date; and
9. Require and keep only the kinds of individual identifying information that is necessary for University purposes.

4.5 Additional Identity Theft Prevention Measures

4.5.1 Hard Copy Distribution

Each employee and contractor performing work for the University will comply with the following procedures:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with identifying information will be locked when not in use.
2. Storage rooms containing documents with identifying information and record retention areas will be locked at the end of each workday or when unsupervised.
3. Desk workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing identifying information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing identifying information are discarded, they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense-approved shredding device. Locked shred bins are labeled "Confidential paper shredding and recycling."

4.6 Program Administration

4.6.1 Oversight

The responsibility for developing, implementing and updating this Program lies with the program administrator designated by the Chancellor. The program administrator shall be responsible for ensuring appropriate training of University 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.

4.6.2 Staff Training

University employees responsible for implementing the Program shall be trained 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.

4.6.3 Reports

Appropriate staff shall report to the program administrator at least annually on compliance with this Program. The report shall address matters such as the effectiveness of the policies and procedures of the University in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and the University's response; and recommendations for material changes to the Program.

4.6.4 Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more covered accounts, the University will take the following steps to ensure the service provider performs its obligations in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft, including the following:

1. Require, by signed contract, that service providers have such policies and procedures in place; and
2. Require, by signed contract, that service providers review the University's Program and report any red flags to the program administrator.

4.6.5 Program Updates

The program administrator shall review and update this Program at least annually to reflect changes in risks to individuals and the University from identity theft. In doing so, the program administrator shall 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.

5 Additional References

This Program incorporates by reference the following policies and procedures:

1. Policy on the Use of Computers and Data Communication
2. Computer Systems Security Policy
3. Remote Access Policy
4. Trusted Access Policy
5. Network Risk Assessment Policy
6. Virtual Private Network (VPN) Policy
7. Wireless Networking Policy
8. Wireless to Trusted Network Policy
9. Statement of Confidentiality

6 Authority

16 CFR Part 681

Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159

North Carolina General Statutes, Chapter 75, Article 2A

7 Contact Information

8 Original Effective Date

9 Revision Dates