Wake Forest University

Identity Theft Prevention Program

Effective May 1, 2009

I. GENERAL

It is the policy of Wake Forest University (“University”) to comply with the Federal Trade Commission's (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. In accordance with the Red Flags Rule, the University is required to develop and implement a written Identity Theft Prevention Program (“Program”). After consideration of the size and complexity of the University's operations and account systems, and the nature and scope of the University's activities, the University, with the approval of the Audit & Compliance Committee of the Wake Forest University Board of Trustees, has adopted the following Program, effective May 1, 2009.

II. IDENTITY THEFT PREVENTION PROGRAM

A. Definitions

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

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

“Covered Account” is an account the University offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, including student accounts or loans that are administered by the University. A “covered account” also includes any other account that the University offers or maintains for which there is a reasonably foreseeable risk to students or others or to the safety and soundness of the University’s business from Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

“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 University is required to establish an “Identity Theft Prevention Program” that 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;

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 associated with Identity Theft.

III. IDENTIFYING RED FLAGS

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open accounts, methods it provides to access accounts, and its previous experiences with Identity Theft. The University has identified the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit 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.

B. 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 information that University has about a student or other individual; and

4. Application that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information provided by the individual (example: inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (for example, an address not matching an address on a loan application);

3. Identifying information presented that is the same as information shown on other applications or documents that were found to be fraudulent;

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. Social security number presented that is the same as one given by another student or other individual;

6. An address or phone number presented that is the same as that of another person;

7. An individual fails to provide complete personal identifying information on an application when reminded to do so; and

8. An individual’s identifying information is not consistent with the information that is on file for that individual.

D. Suspicious Covered Account Activity or Unusual Use of Account

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 the 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 student account information.

E. Alerts from Others

1. Notice to the University from a student, Identity Theft victim, law enforcement or other person that the University has opened or is maintaining an account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS

A. Student Enrollment

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

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 the time the student identification card is issued.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of individuals requesting information (in person, via telephone, via facsimile, via email);

2. Verify the validity of requests to change billing addresses by mail or email

3. Verify changes in banking information given for billing and payment purposes.

4. Verify the identity of individuals requesting to change a password.

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 or background report is sought, the University follow the requirements of the University’s “PRE-EMPLOYMENT DRUG SCREENING, BACKGROUND CHECKS, AND VERIFICATION OF PRIOR EMPLOYMENT” policy to assist in identifying address discrepancies.

V. RESPONDING TO RED FLAGS

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 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 for whom a credit report was run;

3. Change any passwords or other security devices that permit access to Covered Accounts;

4. Not open a new Covered Account;

5. Provide the student with a new student identification number;

6. Notify the Program Administrator for determination of the appropriate step(s) to take;

7. Notify law enforcement;

8. File or assist in filing a Suspicious Activities Report (“SAR”); or

9. Determine that no response is warranted under the particular circumstances.

IV. PROTECTING STUDENT 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 with respect to its internal operating procedures to protect identifying information and to minimize the risk of Identity Theft:

1. Ensure that any website maintained by the University is secure or provide clear notice that the website is not secure;

2. Ensure complete and secure destruction of paper documents and electronic files containing account information when a decision has been made to no longer maintain such information;

3. Ensure that computers or other electronic devices with access to Covered Account information are password protected;

4. Minimize the use of social security numbers;

5. Ensure computer virus protection is up to date; and

6. Require and keep only the kinds of information that are necessary for University purposes.

VII. ADMINISTERING THE PROGRAM

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the individual or committee designated by the President of the University (the “Program Administrator”). The Program Administrator will 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.

B. Staff Training and Reports

University employees 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. University employees shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University’s failure to comply with this Program. At least annually, or as otherwise requested by the Program Administrator, University 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 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 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 University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider

relationship.

3. To ensure contractual obligations are met, advise the Program Administrator when a service provided is engaged

D. Program Updates

The Program Administrator will periodically review and update this Program to reflect changes in risks associated with Identity Theft. In doing so, the Program Administrator will consider the University's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, 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 Committee will update the Program.