Program Adoption

As a best practice and using as a guide the Federal Trade Commission’s (“FTC”) Red Flags Rule, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, The University of North Carolina at Greensboro (“University”) developed this Identity Theft Prevention Program (“Program”). This Program was developed with oversight and approval of the University Board of Trustees. 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 Board of Trustees determined that this Program was appropriate for the University, and therefore approved this Program on April 16, 2009.

The purpose of the program is to detect, prevent and mitigate identity theft in connection with any covered account. This program envisions the creation of policies and procedures in order to achieve these goals.

Definitions

“Account” means a continuing relationship established by a person with the University to obtain a product or service for personal, family, household or business purposes.

“Covered Account” means

- Any accounts that constitute a continuing financial relationship between the University and a person for a service, or that are designed by their nature to permit multiple payments or transactions between the University and a person for a service. These types of accounts include; Perkins loan accounts, Institutional loan accounts, internal tuition payment plan accounts, and tuition payment plan accounts administered by the University’s payment plan service provider.
- Any other account the University offers or maintains for which there is a reasonably foreseeable risk to holders of the account or to the safety and soundness of the University from identity theft, such as use of consumer reports for employee background checks

“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:

- 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
• individual identification number
• bank or other financial account routing code

* These items are also considered public or directory information governed by other campus policies.
** Usage of these numbers at UNCG, (University ID#, ID Card #, and internal database keys) are governed by other campus policies as well.

“Identity Theft” means a fraud committed or attempted using the Identifying Information of another person without authority.

“Identity Theft Prevention Committee ("the Committee")” means the committee designated with primary responsibility for oversight of the Program.

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

“Service Provider” means a person or entity that provides a service directly to the University.

Identification of Red Flags

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 such as: individual identification, caller authentication, third party authorization, and address changes.

The University identifies the following Red Flags in each of the listed categories:

• Notifications and Warnings from Consumer Reporting Agencies
  o Report of fraud accompanying a credit report;
  o Notice or report from a credit agency of a credit freeze on an applicant;
  o Notice or report from a credit agency of an active duty alert for an applicant;
  o Receipt of a notice of address discrepancy in response to a credit report request; and
  o Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity.

• Suspicious Documents
  o Identification document or card that appears to be forged, altered or inauthentic;
  o Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document;
• Other document with information that is not consistent with existing individual information; and
• Application for service that appears to have been altered or forged.

• Suspicious Personal Identifying Information
  
  • Identifying Information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);
  • Identifying Information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application);
  • Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;
  • Identifying Information presented that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);
  • Social security number presented that is the same as one given by another individual;
  • A person fails to provide complete personal Identifying Information on an application when reminded to do so; and
  • A person’s Identifying Information is not consistent with the information that is on file for the individual.

• Suspicious Covered Account Activity
  
  • Change of address for an account followed by a request to change the individual’s name;
  • Payments stop on an otherwise consistently up-to-date account;
  • Account used in a way that is not consistent with prior use;
  • Mail sent to the individual is repeatedly returned as undeliverable;
  • Notice to the University that an individual is not receiving mail sent by the University;
  • Notice to the University that an account has unauthorized activity;
  • Breach in the University’s computer system security; and
  • Unauthorized access to or use of individual account information.

• Alerts from Others
  
  • Notice to the University from an individual, Identity Theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detection of Red Flags

• Student Enrollment

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:
• Require certain Identifying Information such as name, date of birth, academic records, home address or other identification; and
• Verify the individual’s identity at time of issuance of individual identification card (review of driver’s license or other government-issued photo identification).

• Existing Accounts

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:

• Verify the identification of individuals if they request information (in person, via telephone, via facsimile, via email);
• 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
• Verify changes in banking information given for billing and payment purposes.

• 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, University personnel shall take the following steps to assist in identifying address discrepancies:

• 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
• In the event that notice of an address discrepancy is received, verify that the credit 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.

Response to Red Flags

• Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect individuals and the University from damages and loss. The employee will follow the department’s protocol in responding to the situation and notifying those individuals that need to participate in the evaluation and resolution.

• If a transaction is determined to be fraudulent, appropriate actions must be taken by the responsible department immediately. Actions may include:

  • Canceling the transaction;
  • Notifying and cooperating with appropriate law enforcement;
  • Determining the extent of liability of the University; and
  • Notifying the actual individual upon whom fraud has been attempted.
• The department involved in detecting the fraudulent activity must gather all related documentation, write a description of the situation, and report the information to the committee promptly if the fraudulent activity is a major and continuing threat, or at least annually if the fraudulent activity is not a major or continuing threat.

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, depending on their determination of the degree of risk posed by the Red Flag:

• Prevent and Mitigate
  - Continue to monitor a Covered Account for evidence of Identity Theft;
  - Contact the individual or applicant (for which a credit report was run);
  - Change any passwords or other security devices that permit access to Covered Accounts;
  - Refuse to open a new Covered Account;
  - Provide the individual with a new individual identification number;
  - Notify the Committee for determination of the appropriate step(s) taken or that need to be taken;
  - Notify law enforcement;
  - File or assist in filing a Suspicious Activity Report (“SAR”) with the Financial Crimes Enforcement Network, United States Department of the Treasury or other relevant law enforcement agency; or
  - Determine that no response is warranted under the particular circumstances.

• 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 with respect to its internal operating procedures to protect individual Identifying Information:

  - Ensure that websites providing access to covered accounts are secure;
  - Ensure complete and secure destruction of paper documents and computer files containing individual account information in accordance with UNCG records retention guidelines;
  - Ensure that office computers with access to Covered Account information are password protected;
  - Ensure that laptops are password protected;
  - Avoid unnecessary use of social security numbers;
  - Ensure the security of the physical facility that contains Covered Account information;
  - Ensure that transmission of information is limited and encrypted when necessary;
  - Ensure computer virus protection is up to date; and
  - Require and keep only the kinds of individual information that are necessary for University purposes in accordance with UNCG records retention guidelines.
University Policy requires that data that is classified as Restricted in the Data Classification Policy be stored on ITS network storage facilities, not on local hard drives or media.

Additional Identity Theft Prevention Measures

- Hard Copy Distribution

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

- Physical security will be maintained over documents containing Identifying Information related to covered accounts. Examples include keeping offices locked after hours and locking rooms and files when staff are not present.
- Desks, 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.
- Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas, which contain identifying information, will be erased, removed, or shredded when not in use.
- When documents containing Identifying Information are discarded, they will be shredded timely.

- Other Policies and Procedures

This Program incorporates by reference the following internal policies and procedures:

- Information Technology Services policies concerning computer use and electronic records are located at the following URL http://its.uncg.edu/Technology_Policies/ and are incorporated in this policy by reference.

Program Administration

- Oversight

  Responsibility for developing, implementing and updating this Program lies with the Identity Theft Prevention Committee (“the Committee”). The members of the Committee shall be determined by the Chancellor or another senior administrator designated by the Chancellor. The Committee shall be responsible for reviewing any University staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, and considering periodic changes to the Program.

- Staff Training
The management of those departments responsible for covered accounts will insure that staff playing a key role in identifying, detecting, resolving and reporting identity theft are appropriately trained and updated as necessary in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

- **Reports**

The Management of those departments responsible for covered accounts shall report to the Committee at least annually on compliance by the University 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.

- **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.

  - Require, by signed contract, that Service Providers agree to comply with all applicable federal, state and local statutes, rules and regulations, or similar language.

- **Program Updates**

The Committee shall review and update this Program at least annually to reflect changes in risks to individuals and the soundness of the University from Identity Theft. In doing so, the Committee 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.