NC A&T STATE UNIVERSITY

Policies, Regulations and Rules

History: First Issued: July 1, 2009.

Related Policies:
Information Technology Security Plan
Information Technology Data Management Procedures
Process for Access to Social Security Numbers
Aggie One-Card Policy

Additional References:
FTC Identity Theft Red Flags and Address Discrepancies Rule
UNC-GA Counsel Red Flags Guidance Memorandum and Sample Program
Federal Rules on Customer Identification Programs
Information Security Acknowledgement Forms
North Carolina Identity Theft Protection Act (2005 SB-1048)
Family Educational Rights and Privacy Act (FERPA)

---

1. INTRODUCTION

This Policy is issued to implement compliance with the Federal Trade Commission's (FTC) Identity Theft Red Flags and Address Discrepancies Rule at 16 CFR part 681. The general purpose of the Policy is to detect, mitigate, and prevent identity theft in connection with certain financial accounts maintained at NC A&T State University.

2. DEFINITIONS

Terms used in this Policy are meant to be consistent with the definitions as set forth in 16 CFR part 681, including the following:

2.1 "Covered Account" means

- An account that the University offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, including, but not limited to, extension of credit, debit cards, Perkins Loans, Institutional loans, Health Information Protection Accountability Act (HIPAA) covered accounts, deposit accounts, or scholarship accounts; and

- Any other account that the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks, including, but not limited to, use of consumer reports for employee background checks or applications for credit, or Aggie One-Card accounts.
- The Program Administrator shall maintain the definitive list of "Covered Accounts" at the University, as required by 3.1.2 of this Regulation.

2.2 "Identifying Information" means any information that may be used to identify a specific person in conjunction with the name of the person, including, but not limited to:

- 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
- computer's Internet Protocol address
- bank or other financial account routing code
- student identification number issued by the University

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

2.4 "Notice of Address Discrepancy" means a notice sent by a consumer reporting agency to the university that informs the university of a substantial difference between the address submitted by the University when requesting a consumer report and the address(es) on file with the consumer reporting agency as implemented in compliance with 16 CFR 681.1. "Consumer report" normally means a credit report.

2.5 "Program" means the University's Identity Theft Prevention Program, implemented in compliance with 16 CFR 681.2.

2.6 "Program Administrator" means the individual designated with primary responsibility for oversight of the Program.

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

2.8 "Service Provider" means a person or entity that provides a service directly to the University.

3. PROGRAM ADMINISTRATION

3.1 The Assistant Vice Chancellor for Business and Finance shall be the Program Administrator and shall chair the Red Flag Rules Committee.

The Red Flag Rules Committee shall be appointed by the Chancellor or designee, and shall assist the Program Administrator with the implementation and oversight of the Program. The Program Administrator shall maintain the definitive list of personnel serving as a member of the Red Flag Rules Committee.

The duties of the Program Administrator include:

3.1.2 Implementing and Updating the Program. The Program Administrator shall oversee the implementation and annual update of the Program. The Program Administrator shall maintain the definitive list of Covered Accounts maintained by the University and the definitive list of Red Flags. The Program Administrator shall also determine and maintain instructions providing the appropriate university response(s) to Red Flags.

3.1.3 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.

3.1.4 Periodic Identification of Covered Accounts. On an annual basis the Program Administrator shall oversee a review, as required by section 4.4 of this Regulation, which identifies the risk of Identity Theft and the associated Covered Accounts at the University.

3.1.5 Reports. Appropriate staff shall report to the Program Administrator at least annually on compliance by the University with the 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 Covered Accounts; Service Provider arrangements; significant incidents involving Identity Theft and the University's response; and recommendations for material changes to the Program.

The Program Administrator shall report annually to the Vice Chancellor for Business and Finance concerning the compliance by the University with the Federal Trade Commission's Identity Theft Red Flags and Address Discrepancies rule at 16 CFR part 681.

3.2 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 Program Administrator shall 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.

3.2.1 Require, by signed contract, that Service Providers have appropriate Red Flags and Identity Theft policies and procedures in place or will submit a statement explaining why said provider is not subject to the FTC Identity Theft Red Flags and Address Discrepancies Rule.

3.3 Address Discrepancies. The Program Administrator shall establish procedures to verify addresses and consumer identity upon receipt of a Notice of Address Discrepancy. See "Detection of Red Flags" below.

3.4 University Policies. The Program Administrator shall draft and seek adoption of any university policies that are appropriate to advance the purpose of this Program.

4. IDENTITY THEFT PREVENTION PROGRAM

4.1 Identification of Red Flags

4.1.1 As part of identifying relevant Red Flags, the Program Administrator shall consider the types of Covered Accounts the University offers or maintains the methods to open Covered Accounts, the methods to access Covered Accounts, and the University's previous account experiences with Identity Theft. For example, 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.

4.1.2 Examples of Red Flags.

The following five categories of Red Flags are provided in 16 CFR part 681.2 (the Red Flag rule).

4.1.2.1 Notifications and Warnings from Consumer Reporting Agencies. The following are examples of activity that may be considered a Red Flag:

- A fraud or active duty report accompanies a credit report,
- A notice from a credit agency of a credit freeze on an applicant;
- A notice of address discrepancy in response to a credit report request; and
- A credit report indicates a change in the applicant's usual pattern of activity

4.1.2.2 Suspicious Documents. The following are examples of documents that may be considered a Red Flag:

- An identification document or card that appears to be forged, altered or inauthentic;
- An identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- An identification document containing information not consistent with existing individual information; and
- An application that appears to have been altered or forged.

4.1.2.3 Suspicious Personal Identifying Information. The following are examples of information or instances that may be considered a Red Flag:

- Presented Identifying Information that is inconsistent with other information the individual provides or information from external sources (examples: inconsistent birth dates or addresses);
- Presented Identifying Information that is the same as information shown on other applications that were found to be fraudulent;
- Presented Identifying Information that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);
- A presented social security number that is the same as one given to another individual;
- A presented address or phone number that is the same as that of another person;
- Identifying Information included in a person's file that is not consistent with the information that is on file for the individual; and
- A person fails to provide complete personal Identifying Information on an application when reminded to do so.

4.1.2.4 Suspicious Covered Account Activity. The following are examples of activity that may be considered a Red Flag:

- Change of address for an account followed by a request to change the individual's name or for a replacement or additional card;
- 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 a 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.

4.1.2.5 Alerts from Others. An example of an activity that may be a Red Flag would be a notice to the University from an individual, an identity theft victim, or from a law enforcement agency 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 The requirements and examples contained in sections 4.2.2 and 4.2.3 should be interpreted as general instruction to the Program Administrator and the university personnel implementing this Program. The Program Administrator should supplement this general instruction, as necessary, with separate rules or protocols containing detailed detection procedures. All supplemental rules or protocols shall be maintained as documents separate from this Regulation and shall be maintained by the Program Administrator.

4.2.2 Opening of Covered Accounts. In order to detect Red Flags, university personnel shall obtain and verify the identity of the person opening the account. As part of this process university personnel may:

- Require the person to provide Identifying Information such as name, date of birth, academic records, home address or other identification;
- Verify the individual's identity at time of issuance of individual identification card (review of driver's license or other government-issued photo identification); or
- Use other safeguards appropriate to the situation, such as safeguards of a Customer Identification Program (32 CFR 103.121), as required for each identified account situation.

4.2.3 Existing Accounts. In order to detect Red Flags concerning an existing Covered Account, university personnel shall monitor transactions on the account. As part of this process university personnel may:

- 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;
- Verify changes in banking information given for billing and payment purposes; or
- Use other safeguards appropriate to the situation, such as safeguards of a Customer Identification Program (32 CFR 103.121), as required for each identified account situation.

4.2.3 Consumer ("Credit") Report Requests. In order to detect Red Flags concerning an employment or volunteer position for which a credit or background report is sought, or other situations where the University seeks consumer reports, university personnel shall monitor for address discrepancies. As part of this process university personnel may:

- 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;
- If 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; or
- Use other safeguards appropriate to the situation, such as safeguards of a Customer Identification Program (32 CFR 103.121).

4.3 Response to Red Flags

4.3.1 Once a Red Flag is detected, university personnel must act quickly to protect individuals and the University from damages and loss. The process will be implemented in a hierarchical manner utilizing a combination of existing and newly developed processes and documentation, and shall proceed as follows.

4.3.1.1 Any employee who has notice of a Red Flag should consult existing University business procedures associated with the Covered Account for instructions on mitigation of Identity Theft associated with the identified Red Flag.

4.3.1.2 If the specific identified Red Flag situation is not covered adequately by the existing University business procedures, the employee must gather all related information and documentation, and promptly report and discuss the Red Flag with his/her supervisor or manager for mitigation procedures.

4.3.1.3 If existing University business procedures fail to provide adequate instruction for the manager or supervisor to complete an appropriate mitigating response, then the supervisor or manager should refer to the Identity Theft Prevention Program documentation and instructions concerning how to respond to the specific Red Flag.

4.3.1.4 If the Identity Theft Prevention Program does not provide adequate instruction concerning the particular Red Flag for the manager or supervisor to complete an appropriate response, then the supervisor or manager should promptly contact the Program Administrator and present the gathered information and documentation for mitigation instructions from the Program Administrator.

4.3.1.5 After being contacted concerning a Red Flag, the Program Administrator will investigate further, as warranted, and implement the appropriate response. Responses may include:

- Canceling a fraudulent transaction;
- Notifying and cooperating with appropriate law enforcement;
- Changing passwords or other types of security for the Covered Account in question;
- Declining to open a new Covered Account, or closing an existing Covered Account;
- Notifying the individual to whom the Covered Account is assigned, or an applicant for whom a credit report was received, that security has been compromised or a fraud has been attempted;
- Continuing to monitor a Covered Account for evidence of Identity Theft;
- Filing or assisting in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network, United States Department of the Treasury, and determining whether other federal or state government agencies should be notified of the Red Flag;
- Other prescribed mitigation procedures, or
- Determining that no response is warranted under the particular circumstances.

4.3.2 Any University Department who has notice of a Red Flag shall provide a written description of the Red Flag and the Department's response to the Red Flag. The Program Administrator will provide a standardized template. The Department shall produce and provide this written description only after the Department has responded pursuant to the Program and/or initially contacted the Program Administrator concerning the Red Flag. On a monthly basis the department (manager or supervisor) will provide a summary report of all detected Red Flags and their outcomes and forward this to the Program Administrator. This report will also be defined by the Program Administrator as to form and content.

4.4 Annual Review of the Program.

4.4.1 The Program Administrator shall review this Identity Theft Prevention Program annually and recommend any updates necessary to reflect changes in Identity Theft risks. The review shall consider the University's experience with Identity Theft; changes in the methods of Identity Theft; changes in the methods of detecting, preventing and mitigating Identity Theft; changes in the types of accounts the University maintains, and changes in the University's business arrangements.

4.4.2 If the annual review indicates that a new Covered Account has been created, that an existing account qualifies as a Covered Account, or that an existing account no longer qualifies as a Covered Account, the Program Administrator shall update the definitive list of Covered Accounts to reflect the change(s).

4.4.3 If the annual review indicates that a new Red Flag has been identified, that an existing Red Flag requires changed detection and mitigation procedures, or that an existing Red Flag is no longer relevant and should be deleted, the Program Administrator shall update the definitive list of Red Flags to reflect the change(s).

4.4.4 If the annual review indicates that the instructions concerning the appropriate university response(s) to Red Flags need to be updated or modified, the Program Administrator shall update or modify these instructions as necessary.

4.4.5 As part of the annual review, the Program Administrator shall conduct a risk assessment of the methods used to open a Covered Account, the methods used to access Covered Accounts, and previous account experiences with Identity Theft.