RANDOLPH COMMUNITY COLLEGE
IDENTITY THEFT PROGRAM

I. BACKGROUND

As a result of the increasing instances of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Public Law 108-159. This amendment to the Fair Credit Reporting Act dictated that the Federal Trade Commission (FTC) promulgates rules to address identity theft. The rules promulgated by the FTC (Red Flag rules) requires any financial institution and creditor that holds any type of consumer account or other account for which a potential risk of identity theft exists to create and implement a written Identity Theft Prevention Program in order to tackle identity theft associated with new and existing accounts. This Identity Theft Prevention Program is appropriate to the size and complexity of the college and the nature and scope of the college's activities.

II. PURPOSE

Randolph Community College adopted this Identity Theft Prevention Program to enact reasonable policies and procedures to protect students and college employees from damages associated with the compromise of sensitive personal information.

III. DEFINITIONS

A. **Creditor –** Any organization, including community colleges, which regularly:
1. extends, renews, or continues credit; or
2. arranges for someone else to extend, renew, or continue credit; or
3. is the assignee of a creditor involved in the decision to extend, renew, or continue credit.

B. **Credit -** Deferral of payment of a debt incurred for the purchase of goods services, including educational services.

C. **Covered account –** An account with a creditor used by individuals, families, or households which involves multiple payments to that creditor. Examples includes emergency loan accounts, scholarships which could involve repayment if the terms of the scholarship are not met, and deferred payment accounts approved by a colleges' trustees.

D. **Identifying information –** Information which alone, or in combination with other information, can be used to identify a specific individual. Identifying information includes name, social security number, date of birth, driver's license number, identification card number, employer or taxpayer identification number, biometric

data, unique electronic identification numbers, address or routing code, or certain electronic account identifiers associated with telephonic communications.

E. **Identity theft –** A fraud attempted or committed using identifying information of another person without proper authority.

F. **Red Flag –** A pattern, practice, or specific activity which indicates the possibility of identify theft.

G. **Sensitive information –** Personal information belonging to any student, employee, or other person with whom the college is affiliated.

H. **Service provider –** Person providing a service directly to the financial institution or creditor.

IV. **SCOPE –** Activities in which Randolph Community College is involved in that require compliance with the Red Flag Rules include:

A. Utilization of deferred payment plans as authorized by 23 NCAC 02D.0201(b);

B. Issuance of Financial Aid Awards;

C. Maintaining an account for students from which the student can authorize payments for goods and services like books and food;

D. Using debit card accounts;

E. Persons attempting to access academic or financial information.

V. **IDENTIFICATION OF RELEVANT RED FLAGS –** The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

A. Alerts, notifications, or other warnings received from the Attorney General's Office or consumer reporting agencies. For example:

1. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. The presentation of suspicious documents. For example:

1. Documents provided for identification appear to have been altered or forged.
2. The photograph/physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. The unusual use of, or other suspicious activity related to, a covered account. For example:

1. Any student account is used in a manner commonly associated with known patterns of fraud.
2. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
3. The college is notified that the customer is not receiving paper account statements.
4. The college is notified of unauthorized charges or transactions in connection with a customer's covered account.
5. A customer is attempting to access information about a deceased student.
6. The college is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

VI. DETECTING RED FLAGS

Randolph Community College uses the following methods to detect red flags when opening and maintaining covered accounts:

A. Procedures are in place to verify a person's identity when processing any activity to their account including, but not limited to registration activity, financial aid processing, bookstore transactions, and business office payments/inquiries.

B. Receipt of notifications from service providers of red flag criteria (i.e., discrepancies in social security number to name, address differences, etc.) are disseminated to

specifically identified individuals.

C. Receipt of notification of suspicious activity by student, law enforcement or borrower is disseminated to specifically identified individuals.

D. Equipment inventory coordinator reports that laptop and/or computer equipment with sensitive data has been lost or stolen.

E. Randolph Community College has procedures in place to verify changes to sensitive information (e.g. record name changes, SSN changes, and Campus Cruiser password resets).

F. Randolph Community College performs routine diagnostics on firewalls and the security of electronic data portals.

G. Security scans are done in regular intervals.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

Randolph Community College uses the following methods to prevent and to mitigate identity theft when opening and maintaining covered accounts:

A. Third party agencies that handle sensitive data for the college need to be evaluated no less than annually to ensure that they are in compliance with “red flag rules.”

B. All employees are informed and are expected to adhere to FERPA laws to verify proper identity and non-disclosure of data to unauthorized persons.

C. Personal banking information is only obtained and used by appropriate personnel with PCI compliance being maintained regarding security of personal information.

D. A re-admission process is in place to verify a student’s identity when an account has been inactive for a prolonged period.

E. Students applying for financial aid awards are verified with more than one identifying method to assure that aid is being distributed to the proper person.

F. Procedures are in place for the proper handling of data including electronically saved data on laptops and/or flash drives and data that is accessible remotely. This includes what data should be stored on these devices and what security measures should be taken to prevent loss and/or theft of such data.

G. Randolph Community College has Internal Control Narratives in place which are

reviewed annually to assure the security of personal information.

H. Randolph Community College maintains Payment Card Data Security Standard Compliance on portals where payments are taken electronically in an effort for prevention and mitigation of red flags.

I. Randolph Community College trains employees, then reviews procedures for dealing with sensitive information and with access requests.

J. Randolph Community College reviews internal access to paper, electronic documents and information systems containing sensitive information.

K. Randolph Community College provides regular training to educate employees about risks and liabilities of data loss or theft.

VIII. RESPONDING TO DETECTION OF RED FLAGS

Once a red flag has been detected, Randolph Community College will:

A. Ask for validation and/or supplemental documentation/identification when a student's identity is in question.

B. Check credit card receipts when possible fraudulent charges are reported from a customer's bank statement.

C. Verify original student documents when a discrepancy is reported regarding social security number discrepancies to name and other red flag issues regarding aged accounts.

D. Deny access to information or disable an account pending further investigation and resolution of suspicious activity.

E. Follow-up on reported thefts which possibly involve the compromise of sensitive data.

F. Notify victims of possible identity theft and proper authorities.

G. Develop a plan for using all available media to disseminate information concerning an improper disclosure of sensitive information. The records of current students, former students, and employees should be considered when disseminating the information concerning a breach.

IX. UPDATE OF IDENTITY THEFT PROGRAM

This policy will be re-evaluated at periodic intervals to determine whether all aspects of the program are up to date and applicable in the current business environments, and will be revised as necessary.

X. PROGRAM ADMINISTRATION

A. Program Oversight

1. Randolph Community College has designated the Director Financial Services to be responsible for the oversight, development, implementation, and administration of the Identify Theft Prevention Program.
2. A representative has been assigned from each high-risk area to identify what red flags might exist at the college.

B. Staff Training

1. Staff training shall be conducted for all employees for whom it is reasonably foreseeable that they may come in contact with accounts or personally identifiable information.
2. The HR Office/Employee Professional Development Committee is responsible for ensuring identity theft training for all requisite employees.
3. Employees must receive annual training in all elements of this identity theft program.
4. Additional training will be provided as changes to the program are made.

C. Oversight of Service Providers

Randolph Community College assumes the responsibility of ensuring that the activities of all service providers are conducted in accordance with reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft.