5-21 Identity Theft Prevention 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 our size and complexity and the nature and scope of the college's activities.

II. PURPOSE

College of The Albemarle adopts this Identity Theft Prevention Program to enact reasonable policies and procedures to protect college employees, students, contractors and the college from damages associated with the compromise of sensitive personal information. This Program is intended to minimize the potential to steal the identity of someone associated with the college but also to prevent the college of being a source of false identity creation.

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. **Customer –** an employee, a student, a contractor (could be business or professional service agreement)

D. **Covered account –** An account that permits multiple transactions or poses a reasonable foreseeable risk of being used to promote an identity theft. Examples include scholarships which could involve repayment if the terms of the scholarship are not met, deferred payment accounts approved by colleges trustees, student accounts, email accounts, and Datatel accounts.

E. **Financial institution –** Typically a bank, credit union, or other entity that holds for an individual an account from which the owner can make payments, and transfers.

F. **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, college or taxpayer identification number, unique electronic identification numbers, address or routing code, or certain electronic account identifiers associated with telephonic communications.

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

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

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

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

IV. SCOPE – Activities College of The Albemarle are involved that require compliance with the Red Flag Rules include, but not limited to:

A. Utilization of deferred payment plans as authorized by 1E SBCCC 200.2(b);

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

C. Using debit/credit card accounts;

D. Maintaining covered accounts for employees, students, and contractors;

E. Persons attempting to access academic or financial information.

V. IDENTIFICATION OF RELEVANT RED FLAGS

Red Flag Category	Examples of Red Flags
Alerts, notifications, or other warnings received from the Attorney General's Office, consumer reporting agencies, service providers, such as fraud detection services, or other entities used to collect data	A consumer reporting agency issues a fraud or active duty alert.
	A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
	A consumer reporting agency provides a notice of address discrepancy.
	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: 1) A recent and significant increase in the volume of inquiries; 2) An unusual number of recently established credit relationships; 3) A material change in the use of credit, especially with respect to recently established credit relationships; or 4) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
The presentation of suspicious documents	Documents provided for identification appear to have been altered or forged.
	The photograph/physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
	The Social Security Number has not been issued, or is listed on the Social Security Administration's Death Master File.
	A report from with Homeland Security

Red Flag Category	Examples of Red Flags
	indicates inconsistencies to what has been reported to the college.
	Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
	Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
	An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
The unusual use of, or other suspicious activity related to, a covered account	Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
	Any student account is used in a manner commonly associated with known patterns of fraud patterns. For example: The customer fails to make the first payment or makes an initial payment but no subsequent payments.
	A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: a. Nonpayment when there is no history of late or missed payments; b. A material increase in the use of available credit; c. A material change in purchasing or spending patterns; d. A material change in electronic fund transfer patterns in connection with a deposit account; or e. A material change in telephone call patterns in connection with a cellular phone

Red Flag Category	Examples of Red Flags
	account.
	A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors
	Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
	The college is notified that the customer is not receiving paper account statements.
	The college is notified of unauthorized charges or transactions in connection with a customer's covered account.
	A customer initiates multiple address changes over a short period of time.
	A customer is attempting to access information about a deceased student.
	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.
Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the college	A student, borrower, law enforcement personnel or service provider notifies the college of unusual activity related to a covered account. This includes discrepancies in the social security number to a student's name (provided typically by the NC Department of Revenue from debt set-off); address is not a valid address (provided typically by the NC Attorney General's Office), and/or payment plan provider having a discrepancy of data between college and responsible party.
	A student or customer does not know personal information that they should know, i.e. social security number, date of birth, student identification number.

Red Flag Category	Examples of Red Flags
Requests for access to information	A student attempts to change his or her address if an account for that student has been inactive for a prolonged period of time.
Students returning to school after a long period of time	A student wishes to register for courses and/or apply for financial aid when that student's account has been inactive for a prolonged period of time.
	All students that have been inactive for over 5 years are placed in a readmit hold status in the system and must be readmitted only after a current admissions application is received.
Student registration at multiple campus locations	COA will perform verifications of students when registering to be assured that the correct student is being registered for courses. Examples: Register for a class: Picture ID and SSN required. Register for a class with another student with same name. Picture ID, SSN, date of birth, address, and phone number required. _____ To initiate a name change student must present a Social Security card with the student's new name.

VI. DETECTING RED FLAGS/IDENTITY THREATS

A. The college collects, uses, and/or discloses identifying information as permitted by applicable laws and institutional policies and only in furtherance of legitimate college business.

B. Procedures should be in place to verify a person's identity when processing any activities such as account payments and account inquiries.

C. Receipt of notifications from service providers of red flag criteria (i.e. discrepancies in social security number to name, address differences, etc.) should be disseminated to proper personnel.

D. Receipt of notifications of suspicious activity by student, law enforcement, employee or borrower should be disseminated to proper personnel.

E. The Department of Education randomly selects students for financial aid verification. These students are verified by financial aid staff or through an approved third party.

F. Any report by an employee that laptops and/or computer equipment with sensitive data have been lost or stolen need to be addressed by proper personnel.

G. The college should appropriately process changes to sensitive information (i.e. record name changes, social security number changes, etc.)

H. The college should perform routine diagnostics on firewalls and the security of electronic data portals.

I. Security scans should be done at regular intervals to detect any possible breaches.

J. The college must caution employees to be aware of their surroundings when talking with students or discussing a student with another college employee.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

A. Employee Accounts

a. Documentation will be required to verify employee identity prior to processing for employment and/or payment. Any discrepancies of information should be addressed by college

personnel through a verification process assuring the prospective employee is indeed who they claim to be.

B. Forms, Documents, and Records

a. Any form that requires a personal identifier must label impute fields appropriately and avoid the use of social security numbers. Forms which require that SSNs be used under applicable state and federal laws are exempt.

b. Documents that include identifying information must be stored in a secure place. When possible, records containing identifying information, including back-ups, should be protected during storage by encrypting the numbers in electronic records or storing records in other media forms in locked cabinets.

c. When possible, printed reports and other documents should not list identifying information. If identifying information needs to be included in printed documents, such documents should be accessible only to employees that require the information for the performance of their duties.

C. Training of Employees

a. COA should have regular, mandatory staff meetings to educate employees about risks and liabilities of data loss or theft.

b. COA will train appropriate employees, then review and test procedures for dealing with sensitive information and with access requests.

c. COA should review internal access to paper, electronic documents and information systems containing sensitive information.

VIII. RESPONDING TO DETECTION OF RED FLAGS

Once potentially fraudulent activity is detected, it is essential to act quickly as a rapid appropriate response can protect customers and the college from damages and loss.

a. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Take this information and present it to the Chief Financial Officer.

b. The designated program representative will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

c. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

- Cancel the transaction
- Notify and cooperate with appropriate law enforcement
- Determine extent of liability to college

d. Notify actual customer that fraud has been attempted. Receipt of notification of suspicious activity by student, law enforcement or borrower should be disseminated to specifically identified individuals.

e. As appropriate the following additional items should be considered.

1. Ask for validation and/or supplemental documentation/identification when a student's identity is in question.
2. Check credit card receipts when possible fraudulent charges are reported from a customer's bank statement.
3. Verify original student documents when a discrepancy is reported regarding social security number discrepancies to name and other red flag issues regarding aged accounts.
4. Deny access to information or disable an account pending upon further investigation and resolution of suspicious activity.

5. Follow-up on reported thefts which possibly involve the compromise of sensitive data.
6. Develop a plan for notifying victims of possible identity theft and proper authorities. Receipt of notifications from service providers of red flag criteria (i.e., discrepancies in social security number to name, address differences, etc.) should be disseminated to specifically identified individuals.
7. 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

The Chief Financial Officer will evaluate and update as necessary the Identity Theft Prevention Program on an annual basis or as deemed appropriate by senior administration or other factors such as current issues, advances in technology, or other related policies.

X. PROGRAM ADMINISTRATION

A. **Program Oversight** - The Board of Trustees is required to review and approve an Identity Theft Prevention Policy. The Board of Trustees designates that the Chief Financial Officer be designated as the Identity Theft Prevention Officer who is responsible for the oversight, development, implementation, and administration of the Identity Theft Prevention Program.

B. **Staff Training –** The college will ensure adequate staff training considering the needs of our faculty and staff, multiple records and various locations through professional development, staff meetings, or other methods as established by Deans/Vice Presidents/Chairs/Directors.

C. **Oversight of Service Providers** It is the responsibility of the college to ensure that the activities of all Service Providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of

identity theft. A Service Provider that maintains its own Identity Theft Prevention Program, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements. Any specific requirements should be specifically addressed in the appropriate contract arrangements.