DAVIDSON-DAVIE COMMUNITY COLLEGE

Business Services

IDENTITY THEFT

POLICY 6.3.10

POLICY OVERVIEW

This Policy is intended to meet the requirements of the FTC "Red Flag Rule." Identity theft is a fraud committed or attempted using the identifying information of another person without that person's authority. The College shall undertake reasonable measures to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," and to establish a system for reporting a security incident.

DEFINITIONS

A. Covered Account – A covered account is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

B. Creditor – A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college is a "creditor" are:

1. Participation in the Federal Perkins Loan program;
2. Participation as a school lender in the Federal Family Education Loan Program;
3. Offering loans to students, faculty or staff;
4. Offering a plan for payment of tuition or fees throughout the semester rather than requiring full payment at the beginning of the semester.

C. Identifying Information – Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person including: photo, 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, routing code or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

D. Red Flag – A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

E. Security Incident – A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

IDENTIFICATION OF RED FLAGS

Broad categories of "Red Flags" include the following:

A. Alerts – alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.

B. Suspicious Documents – such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.

C. Suspicious Personal Identifying Information – such as discrepancies in address, Social Security Number or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.

D. Unusual Use or Suspicious Account Activity – such as material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges.

E. Notice from Others Indicating Possible Identify Theft – such as the College receiving notice from a victim of identity theft, law enforcement or another account holder reports that a fraudulent account was opened.

DETECTION OF RED FLAGS

College employees shall undertake reasonable diligence to identify Red Flags in connection with the opening of covered accounts as well as existing covered accounts through such methods as:

A. Obtaining and verifying identity;

B. Authenticating customers; and

C. Monitoring transactions.

A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the College or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags.

COLLEGE REQUIREMENTS

During its 2005 session, the General Assembly of North Carolina enacted Senate Bill 1048, titled the Identity Theft Protection Act of 2005. This law is designed to protect individuals from identity theft, and specifies procedures that businesses must follow in order to protect an individual's identity. As such, the following College policy regarding the handling of sensitive personal information is intended to adhere to that law. Exceptions to this are provided in subsections (c) and (d) of G.S. § 132-1.10.

COLLEGE PROCEDURE FOR OBTAINING SOCIAL SECURITY OR EMPLOYEER TAXPAYER IDENTIFICATION NUMBERS

The College has identified the following authorized instances to collect a social security or employer taxpayer identification number:

- Application for admission to the College
- Registration/application for continuing education courses
- Application for financial aid
- Application for employment
- Application for new vendor status
- As required by federal, state, and local governmental agencies

The College must collect the social security or employer taxpayer identification numbers in order to meet federal, state, and local government reporting requirements. For example, student social security numbers are required to be reported on annual Internal Revenue Service Form 1098-T, which shows total tuition paid by each year by students. The College may collect, use, or release the identification for the following purposes:

1. Internal verification or administrative purposes within the College.
2. Open an account or the provision of payment for a product or service authorized by an individual.
3. Establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the identification number for the purpose of obtaining a credit report.
4. Investigate or prevent fraud, conduct background checks, conduct social or scientific research, or collect a debt.
5. Adhere to a court order, warrant subpoena, or when otherwise required by law.
6. Adhere to requests from a federal, state, or local government, including a law enforcement agency, court, or their agents or assigns.

DESTRUCTION OF PERSONAL INFORMATION RECORDS

The College routinely destroys appropriate records after they have reached a certain age pursuant to the NCCCS Records Retention & Disposition Schedule. In order to protect against unauthorized access to or use of this information, the College shall destroy such records that contain personal information by burning, pulverizing, or shredding the documents. In the case of electronic information, the College requires the destruction or erasure of electronic media and other non-paper media containing personal information so that the information cannot practicably be read or reconstructed. The College may, after due diligence, enter into a written contract with, and monitor compliance by, another party engaged in the business of record destruction to destroy personal information in a manner consistent with the procedures listed above.

SECURITY INCIDENT REPORTING

College employees who believe that a security incident has occurred shall immediately notify his/her appropriate supervisor and the Vice President and Chief Financial Officer. Upon review of the incident, the Vice President and Chief Financial Officer shall determine what steps may be required to mitigate any issues that arise in the review. In addition, referral to law enforcement may be required.

If there is a security breach, the College shall comply with all notice requirements contained in N.C.G.S. § 75-65[1].

TRAINING

All College employees who process any information related to a covered account shall receive annual training and this Policy shall be reviewed annually.

Adopted: April, 2020

Legal Reference: Fair and Accurate Credit Transactions of 2003; FTC Regulations – Red Flag Rule; N.C.G.S. § 75-65; N.C.G.S § 132-1.10; N.C. IDENTITY THEFT PROTECTION ACT OF 2005;

[1] Public entities are not subject to the notice provisions of N.C.G.S. §75-65, however, we have typically recommended Colleges follow the notice provisions outlined in the statute. We can discuss the pros and cons if you would like to consider removing this provision.