NORTHEAST COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE NUMBER: AP-3511.4

FOR POLICY NUMBER: BP – 3511

IDENTITY THEFT PREVENTION

1. PROCEDURE SUMMARY STATEMENT

To describe the protocol that complies with a federal mandate relating to identity theft. This mandate requires creditors who have entered into business arrangements that meet the definition of a "covered account" to establish an identity theft prevention program.

2. DEFINITIONS

2.1 Identity Theft – a fraud committed or attempted using the identifying information of another person without authority.

2.2 Identifying Information – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. For example:

2.2.1 Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification;

2.2.2 Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

2.2.3 Unique electronic identification number, address, or routing code; and

2.2.4 Telecommunication identifying information or access device (as defined in 18 USC 1029(e), as the same may from time to time be amended).

2.3 Account – a continuing relationship established by a person with the College to obtain a product or service for personal, family, household, or business purposes including:

2.3.1 An extension of credit, such as the purchase of property or services involving a deferred payment; and

2.3.2 A deposit account.

2.4 Covered Account –

2.4.1 As defined by the Federal Trade Commission (FTC), an account the College offers or maintains that involves or is designed to permit multiple payments or

transactions. Examples include certain student loan accounts, and accounts for the payment of tuition, fees or other charges over time; and

2.4.2 Any other account that the College or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2.5 Customer – a person that has a covered account with the College.

2.6 Red Flag – a pattern, practice, or specific activity that indicates the possible existence of identity theft.

2.7 Service Provider – an individual or organization that provides a service directly to the College.

3. PROCEDURE

3.1 Approval and Management; Program Administration; Training; Annual Report

3.1.1 The College's Vice President of Finance and Facilities will be responsible for overall program management and administration. The Vice President of Finance and Facilities or designee shall be responsible for the provision of appropriate identity theft training for relevant college employees and for providing reports and periodic updates to the Cabinet on an annual basis.

3.1.2 The annual report shall evaluate issues such as the effectiveness of the policies and procedures for addressing the risk of identity theft with respect to covered accounts, oversight of service providers, significant incidents involving identity theft and the College's response, and any recommendations for material changes to the program. As part of the review, red flags may be revised, replaced, or eliminated. Defining new red flags may also be appropriate.

3.2 Transactions at Risk

3.2.1 The College has determined that the following are "covered accounts" and thus subject to the identity theft prevention policy:

3.2.1.1 Student accounts utilizing either an internal college payment plan or an approved external third party servicer payment plan.

3.2.1.2 The College's emergency (short term) loan program.

3.2.2 The College shall review the guidelines that contain potential red flags in Appendix A to part 681 of Title 16 in the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, and will continue to do so as the same may from time to time be amended.

3.3 Risk Assessment

3.3.1 The College will consider the following risk factors in identifying red flags for covered accounts, if appropriate:

3.3.1.1 The types of covered accounts the College offers or maintains;

3.3.1.2 The methods the College provides to open covered accounts;

3.3.1.3 The methods the College provides to access covered accounts; and

3.3.1.4 The College's previous experience with identity theft.

3.3.2 The College shall incorporate relevant red flags from sources such as:

3.3.2.1 Incidents of identity theft that the College has experienced or that have been experienced by other colleges and universities;

3.3.2.2 Methods of identity theft identified by the College or other creditors that reflect changes in identity theft risks; and

3.3.2.3 Applicable supervisory guidance.

3.3.3 The College shall include relevant red flags from the following categories, if appropriate:

3.3.3.1 Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

3.3.3.2 The presentation of suspicious documents;

3.3.3.3 The presentation of suspicious personal identifying information, such as a suspicious address change;

3.3.3.4 The unusual use of, or other suspicious activity related to, a covered account; and

3.3.3.5 Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

3.3.4 The College shall attempt to detect relevant red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

3.3.4.1 Obtaining identifying information about, and verifying the identity of, a person opening a covered account.

3.3.4.2 Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

3.3.5 The College shall consider the following instances as red flags:

3.3.5.1 Notifications or warnings from a consumer reporting agency; and

3.3.5.2 Suspicious documents

3.3.5.2.1 The photograph, physical description, or other information on the identification is not consistent with the appearance of, or information provided by the customer presenting the identification.

3.3.5.2.2 Documents provided for identification appear to have been altered or forged.

3.3.5.2.3 Other information on the identification is not consistent with readily accessible information that is on file with the College.

3.3.5.2.4 An application appears to have been altered or forged, or given the appearance of having been destroyed and reassembled.

3.3.5.3 Suspicious Personal Identifying Information

3.3.5.3.1 Personal identifying information provided is inconsistent when compared against external information sources used by the College. For example:

3.3.5.3.1.1 The address does not match any address in the consumer report; or

3.3.5.3.1.2 The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

3.3.5.3.2 Personal identifying information is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the Social Security Number range and date of birth.

3.3.5.3.3 Personal identifying information provided is associated with known or suspected fraudulent activity as indicated by internal or third-party sources used by the College.

The Social Security Number, address, or telephone number provided is the same as that of other customers.

3.3.5.3.4 The customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

3.3.5.3.5 Personal identifying information provided is not consistent with personal identifying information that is on file at the College.

3.3.5.3.6 If the College uses challenge questions, the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

3.3.5.4 Unusual use of, or Suspicious Activity Related to, the Covered Account

3.3.5.4.1 A covered account is used in a manner that is not consistent with established patterns of activity on the account, such as:

3.3.5.4.2 A covered account that has been inactive for a reasonably lengthy period of time is used. Determining what is reasonably lengthy should take into consideration the type of account, the expected pattern of usage, and other factors which may be relevant;

3.3.5.4.3 Nonpayment when there is no history of late or missed payments;

3.3.5.4.4 Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account; and

3.3.5.4.5 The College is notified of unauthorized charges or transactions in connection with a customer's covered account.

3.3.5.5 Notice from Customers and Others Regarding Possible Identity Theft in Connection with Covered Accounts Held by the College

3.3.5.5.1 The College is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person, that the College has opened a fraudulent account for a person engaged in identity theft.

3.3.6 Response to Detected Red Flags

3.3.6.1 The program shall provide for appropriate responses to detected red flags in order to prevent and mitigate identity theft. The response of the

College shall be commensurate with the degree of risk posed. Appropriate responses may include, but not be limited to:

3.3.6.1.1 Monitoring a covered account for evidence of identity theft;

3.3.6.1.2 Contacting the customer;

3.3.6.1.3 Changing passwords, security codes, or other security devices that permit access to a covered account;

3.3.6.1.4 Canceling the transaction;

3.3.6.1.5 Reopening a covered account with a new account number;

3.3.6.1.6 Not opening a new covered account;

3.3.6.1.7 Closing an existing covered account;

3.3.6.1.8 Notifying and cooperating with appropriate law enforcement; or

3.3.6.1.9 Determining no response is warranted under the particular circumstances.

3.3.7 Updating the Program

3.3.7.1 The program shall be re-evaluated and updated periodically to reflect changes in risks to customers or the safety and soundness of the College based on factors such as:

3.3.7.1.1 The College's experience with identity theft;

3.3.7.1.2 Changes in methods of identity theft;

3.3.7.1.3 Changes in methods to detect, prevent, and mitigate identity theft;

3.3.7.1.4 Changes in the types of accounts that the College offers or maintains; or

3.3.7.1.5 Changes in the business arrangements of the College, including service provider arrangements.

3.3.7.2 The reviews shall include an assessment of which accounts are covered by the program, and the risk of identity theft with respect to each type of covered account.

3.3.8 Oversight of Service Providers

3.3.8.1 It shall be the responsibility of the College to ensure that the activity of a service provider, who is engaged by the College to perform an activity in connection with covered accounts, is conducted 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 that is consistent with the policy of the College and the federal law and regulations may be considered to be meeting these requirements.

4. APPLICABILITY

N/A

ISSUE DATE: 03/27/2019
EFFECTIVE DATE: 03/27/2019
REVISION DATE(S): 05/14/2009 (item #10440); 12/01/2014; 03/27/2019
PRIOR POLICY/PROCEDURE NUMBER: 2720; AP-3250.0
SCHEDULE FOR REVIEW: 2024
DIVISIONS/DEPARTMENT RESPONSIBLE FOR REVIEW & UPDATE: Finance and Facilities
SPONSORING DIVISION/DEPARTMENT: Finance and Facilities
LEGAL REFERENCE: Federal Trade Commission's (FTC) Red Flags Rule, Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003
RELATED PROCEDURES/ REFERENCE: AP-3511.0; AP-3511.1; AP-3511.2; AP-3511.3
PROCEDURE KEY WORDS: identity theft; Red Flags Rule; Fair and Accurate Credit Transactions Act of 2003; FACTA