KASKASKIA COLLEGE

IDENTITY THEFT PURSUANT TO RED FLAGS RULE PROCEDURE

Policy Number: 3.7000
Subject Area: Business Services and Finances
Adopted: 12/17/2009
Revised: 12/17/2009

I. DETECTION OF RED FLAGS

The program includes detection of Red Flags on both new and existing accounts.The Program Administrator, along with members of the Red Flag Committee, will develop and implement specific methods and protocols appropriate to meet the goals and requirements of this Program.

New Accounts

- In order to detect any of the Red Flags associated with the opening of a new account, procedures and processes will include appropriate elements from the following steps in order to obtain and verify the identity of the person opening a new account:
  - Require certain identifying documentation and all requested information such as name, date of birth, Social Security Number (SSN), academic records, residential or business address, driver's license or other identification;
  - Review documentation to detect alteration or forgery;
  - Review information and documentation for consistency;
  - Verify the account holder's identity at time of issuance of an identification card (for instance, review a driver's license or other government-issued photo identification card);

Existing Accounts

- In order to detect any of the Red Flags during the use of an existing account, procedures and processes will include appropriate elements from the following steps in order to provide a reasonable assurance of the identity of the person:
  - Verify the identification of account holders if they request information (in person, via telephone, via facsimile, via email)
  - Review documentation to detect alteration or forgery
  - Verify the validity of requests to change billing/payment addresses
  - Verify changes in banking information provided for billing/payment purposes.

II. RESPONDING TO RED FLAGS AND MITIGATING IDENTITY THEFT

- In order to mitigate the risk and impact of an identity theft, procedures and processes will include appropriate elements such as those listed in the following example steps in response to observance or notification of one or more Red Flags. The actual response may vary depending on the nature and degree of risk posed by the Red Flag:
  - Investigate the incident further to verify and gather information
  - Continue to monitor an account for evidence of Identity theft
  - Contact the account holder
  - Change any passwords or other security devices that permit access to accounts
  - Decline opening the new account
  - Close an existing account
  - Reopen an account with a new number
  - Notify law enforcement
  - Determine that no response is warranted under the particular circumstances

III. OVERSIGHT OF THIRD-PARTY SERVICE PROVIDERS

- In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College will 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:
  - Require, by contract, that service providers have such policies and procedures in place.
  - Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship.

IV. TRAINING

- Staff training is required for all employees, officials, and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the College or its customers.
- The Committee will train the Department Head of each office that maintains covered accounts who in turn will be responsible for ensuring that appropriate identity theft training for all requisite employees occur. College employees responsible for implementing the Program shall be trained either by or 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.
- Appropriate staff shall provide regular reports to the Program Administrator on incidents of identity theft, the effectiveness of the Program and the College's compliance with the Program.

V. PROGRAM ADMINISTRATION

- Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the College, headed by the Program Administrator. The Identity Theft Committee will consist of key staff members from the departments of Information Technology, Human Resources, Payroll, Financial Aid, Accounts Receivable, Accounts Payable, the Bookstore, and other appropriate departments, along with the Director of Information Technology acting as the Program Administrator. The Committee will be responsible for implementing an Identity Theft Program, ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances.
- The Committee will review the program and create an annual report, based upon assessing the effectiveness of the College's Identity Theft Program. This review will include an assessment of which accounts are covered by the program, whether additional Red Flags need to be identified as part of the Program, whether training has been implemented, whether training has been effective. In addition, the review will include an assessment of whether mitigating steps included in the program remain appropriate, and/or whether additional steps need to be defined. As part of the report, the Committee will make recommendations for updating or modifying the Program as appropriate.

APPENDIX A

Alerts, Notifications or Warnings from a Consumer Reporting Agency (or Other Service Provider)

- A fraud or active duty alert is included with a consumer report.
- 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 (as defined in § 41.82(b))
- 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 recent and significant increase in the volume of inquiries;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- 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 Kaskaskia College, 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.

Suspicious Personal Identifying Information

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

- The address does not match any address in the consumer report; or
- The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
    - Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
    - Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
- The address on an application is the same as the address provided on a fraudulent application; or
- The phone number on an application is the same as the number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Kaskaskia College. For example:
- The address on an application is fictitious, a mail drop, or a prison
- The phone number is invalid, or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with Kaskaskia College.
- For institutions that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

Shortly following the notice of a change of address for a covered account, we receive a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
- The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
- 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:

- Nonpayment when there is no history of late or missed payments
- A material increase in the use of available credit;
- A material change in purchasing or spending patterns;
- A material change in electronic fund transfer patterns in connection with a deposit account; or
- A material change in telephone call patterns in connection with a cellular phone 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.
    - We are notified that the customer is not receiving paper account statements.
    - We are notified of unauthorized charges or transactions in connection with a customer's covered account.

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 Financial Institution or Creditor

- We are 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.

Approval History: Replaces Identity Theft Pursuant to Red Flags Rule Procedure 4.7 approved December 17, 2009