CMOP 2100

Red Flag Rules

Background

The Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule (Fair and Accurate Credit Transactions Act of 2003 Sections 114 and 315) to be implemented no later than May 1, 2009. Under the Red Flag Rule, financial institutions and creditors with "covered accounts" must have identity theft prevention programs in place for the purposes of identifying, detecting and responding to activities that raise a "Red Flag" with respect to identity theft.

A "Red Flag" is defined as a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of "Red Flag" incidents include presentation of suspicious identity documents or frequent address changes.

The Vice President for Finance & Business and Vice President for Human Resources shall be responsible for establishing and implementing procedures for identifying and detecting identity theft and red flag rule incidents.
Scope

The activities identified that would come under the Red Flag Rule at Kalamazoo Valley Community College include:

- Payment plans, promissory notes, and tuition delays for covered student accounts and tuition.
- Credit reports for employee hiring process and commercial card issuance.

Definitions

- **Covered Account** – 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 payment plan.
- **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:
    - Offering institutional loans to students or employees;
    - Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester;
    - Payment of employee charges through payroll deduction.
- **Personal Information** – Specific items of personal information including an individual's first name or first initial and his/her last name in combination with any one or more of the following elements, when either the name or the data elements are not encrypted or redacted: Social Security Number, driver's license/State identification card number, health insurance information, medical information, 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.
- **Red Flag** – A pattern, practice, or specific activity that indicates the possible existence of identity theft.
- **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:

- **Alerts** – Alerts, notifications, or warnings from consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.
- **Suspicious Documents** – Documents 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.
- **Suspicious Personal Identifying Information** – Discrepancies in address, Social Security Number, or other information on file (e.g., inconsistent birthdates), an address that is a mail-drop, a prison, or is invalid, an address or telephone number that has previously been identified as fraudulent, 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.
- **Unusual Use or Suspicious Account Activity** – Material changes in payment patterns, notification that the account holder is not receiving mailed statements, mail repeatedly returned as undeliverable, or that the account has unauthorized charges.
- **Notice from others Indicating Possible Identity Theft** – Institution receives notice from victim of identity theft, law enforcement, or another account holder reports that a fraudulent account was opened.
- **Breach** – Breach of College's computer system security, unauthorized access to or use of customer account information.

Detection of Red Flags

Detection of Red Flags in connection with the opening of covered accounts as well as existing covered accounts can be made through such methods as:

- **Obtaining and verifying identity** – Require identifying information such as name, date of birth, address, or other information.
- **Authenticating customers** – Compare information to driver's license, student or employee identification card, or other identification (e.g., passport).
- **Monitoring transactions** – Independently contacting the student or employee, verify validity of request to change billing addresses.

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.

Response to Red Flags

The detection of a Red Flag by an employee shall be reported immediately to theDirector of Public Safety. Based on the type of Red Flag and the degree of risk posed by the Red Flag, the Director of Public Safety or his/her designee will determine the appropriate response which may include one or more of the following actions:

- Contacting the student or employee;
- Changing any passwords or other security devices that permit access to accounts;
- Close an existing account and/or reopen an account with a new number;
- Notify law enforcement; or,
- Determine that no response is warranted under the particular circumstances.

The Director of Public Safety will investigate the threat of identity theft to determine if there has been a breach and will respond appropriately to prevent future identity theft breaches. Additional actions may include notifying and cooperating with appropriate law enforcement and notifying the student or employee of the attempted fraud.

Protecting Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to College accounts, the College will take steps with respect to its internal operating procedures to protect customer identifying information:
• Secure college websites that contain personal information.
• Provide for complete and secure destruction of paper documents and computer files containing customer information.
• Ensure that office computers are password protected and that computer virus protection is up-to-date.

Service Providers

The College remains responsible for compliance with the Red Flag Rule even if it outsources operations to a third party service provider. The written agreement between the College and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate whether the service provider is responsible for notifying only the college of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identity theft.

Agreements may include, but are not limited to, third party collection and billing agencies.

Training

All employees who process any information related to a covered account shall receive training following appointment on the procedures outlined in this document. Refresher training may be provided annually.

Private information will be limited to those employees on campus with a legitimate "need-to-know". Employees who have approved access to the databases understand that they are restricted in using the information obtained only in the conduct of their official duties. The inappropriate use of such access and/or use of administrative data may result in disciplinary action up to, and including, dismissal from KVCC.