

Culver-Stockton College

Red Flag Identity Theft Prevention Program

Effective June 1, 2010

Background

In November 2007, the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration jointly issued a regulation known as the “Red Flags Rule”. This regulation requires all “financial institutions” and “creditors” that contain covered accounts to create an Identity Theft Program. As defined by the FTC, a “creditor” is a business or organization that regularly defers payment for goods or services or provides goods or services and bills customers at a later date. The identity theft program must contain four basic steps: Identifying relevant red flags, detecting red flags, responding to red flags, and administering the program.

A “red flag” is defined as a pattern, practice, or specific activity that indicated the possible existence of identity theft.

For businesses or organizations that are subject to the Red Flags Rule, identity theft programs are required to be in place by December 31, 2010. Culver-Stockton College recognizes that some of its activities are subject to the provisions of the Red Flags Rule and hereby adopts this policy and the following *Red Flag Identity Theft Prevention Program*.

Scope of Red Flag Activities

- Participation in the Federal Perkins Loan Program
- Offering institutional student loans
- Offering institutional computer loans to employees
- Payment plans for covered student accounts
- Background checks in the employee hiring process
- Payment of faculty and staff dining services charges through payroll deduction
- Offering students the ability to charge purchases at the Logo Shop directly to their student accounts

Departments Impacted by Program

The following departments will be impacted by Culver-Stockton College's *Red Flag Identity Theft Prevention Program*:

- Administration and Finance Office
 - Training
 - Address changes, presentation of identification for 1-9 form
 - Background checks
 - Request for payroll documents
 - Computer loan requests
- Financial Aid
 - Address changes
 - EdConnect Loan Files
 - Financial Aid document verification (ISIR)
 - Online Early Estimator
- Registrar
 - Address changes
 - Request for transcripts
- Logo Shop
 - Student purchases that are charged on account
- Admissions
 - Changes to applicant information (online or paper form)
 - Electronic Transcripts
 - Online Confirmation Fee
- Information Technology
 - Password/system access
- Dining Services
 - Faculty/Staff ID cards for payroll deduction of dining service charges
- Student Accounts
 - Address changes
 - Requests for 1098-T documents
 - Payment plans made with students, faculty, or staff
 - Covered accounts of Federal Perkins Loans and institutional loans
 - Wiring Information
- Student Life/Residence Life
 - Changes to medical records
- Advancement
 - Address change
 - Changes in donor information
- Athletics
 - Medical Records
- Career Placement
 - Student Resume Information

Existing Policies and Practices

Many offices at Culver-Stockton College maintain records of students (along with parent information), employees (along with family information), and alumni. These records can be in paper and/or electronic form. The records are safeguarded to ensure the privacy and confidentiality of each of these individuals.

The controls by Culver-Stockton College over privileged information include:

- Students are given the opportunity to release certain information (billing, financial aid, residence life, and registrar) to a third party (parents or grandparents) by signing the FERPA (Family Educational Rights and Privacy Act) release form.
- Access to personal data in the TEAMS Database is restricted to those employees with a need to properly perform their duties. These employees are aware of the procedures dealing with FERPA.
- Financial Aid employees are trained to know FERPA regulations.
- Social Security numbers are not used as primary identification numbers.
- The College is sensitive to personal data, and will not disclose any information unless by written request or a legitimate “need-to-know” basis.
- The College’s official personnel files for all employees are retained in the Administration and Finance Office. Employees have the right to review the materials contained in their personnel file at any time as long as an employee of the Administration and Finance Office is present, and the files do not leave the office.
- The Logo Shop requires students to present their school ID card (which contains a photograph) before any charge on their student account can be made.
- The College ensures that its website is secure with identifying information.
- The College securely destroys paper documents and files containing student or employee information when a decision is made to no longer maintain such information.
- The College’s office computers are secured with password access.
- The College’s virus protection is consistently up-to-date.
- All offices and storage rooms that contain critical information are secured at the end of each workday or when they are unsupervised.
- All student workers are required to sign a Confidentiality Agreement upon being hired which is maintained in the Administration and Finance Office.

- All employees are aware of the importance of confidentiality. Each employee has access to the Faculty/Staff Handbooks, in which it reads:

Employees at Culver-Stockton College are privileged to certain business-related information that is confidential and critical to the College. It is mandatory that this information be used by employees only for the purpose of executing responsibilities on the job. No information that would cause harm to the operations of Culver-Stockton should be discussed with any individual or other entity. In the event of separation, all confidential information, learned or gathered, must continue to be kept confidential.
- The College has policies that address the safeguarding of various forms of confidential information. Those policies include:
 - Internet Policy: Section V, page 8 of the Staff Handbook; Page 94 of the Faculty Handbook.
 - E-mail/Computer and Internet Access: Section V, page 8 of the Staff Handbook; Page 67 of the Faculty Handbook.

Step 1: Identification of Relevant Red Flags

Identification of relevant red flags includes, but is not limited to, the following circumstances:

- Presentation of suspicious documents.
 - Address discrepancy.
 - Name discrepancy on identification.
 - Altered or falsified identification.
 - Description information on ID does not match photo or presenter of the ID.
 - Personal information inconsistent with information already on file.
- Unusual use or suspicious activity related to a covered account
 - Change of address followed by a request to change name.
 - Account activity inconsistent with prior use.
 - Mail sent to a student is consistently returned as “undeliverable”.
 - A student, law enforcement, or someone else notifies the College that an account has unauthorized activity.
 - Duplicate Social Security number.
 - Address or phone number occurring repeatedly for multiple students, employees, alumni/donors.
 - Person making contact is unable to confirm other account information or accurately respond to the challenge questions.
- Notifications and warnings from credit reporting agencies that there is an address discrepancy in response to a credit report request (Parent Plus Loans).

Step 2: Detection of Red Flags

In addition to identifying potential Red Flags, Culver-Stockton College will also perform the following to detect when Red Flags could possibly occur:

- Training staff how to recognize, record, and report suspected red flag activity.
- Ensuring that all requested information to establish an account has been provided and matches other available information.
- Establishing an individual or group of individuals who act as the point of contact for all red flag-related activity by monitoring and reporting the activity.
- Obtaining identifying information about and verifying the identity of newly hired employees, newly enrolled students, etc.
- Monitoring transactions through photo ID (Drivers License/Culver-Stockton College Student ID Card) verification.
- Requiring an alternative identification method if photo ID appears to be altered or forged.
- Rejecting any application for a service or transaction that appears to be altered or forged.
- Verify the identity of individuals requesting a change in name, address, or other account information.

Step 3: Responding to Red Flags

Once red flags have been identified and detected, the College must respond to the situation according to an established plan, and notify the affected parties. Responding to red flags includes the following, which should be performed within 24 hours of detection:

- Once detected, gather all related documentation and write a description of the situation. Present this information to the Chief Financial Officer who will then determine if the transaction is fraudulent.
- Contact the owner of the covered account or the identity theft victim that is being questioned by phone, email, letter, or other source of communication.
- Cancel the transaction.
- Notify the appropriate law enforcement.
- Change any passwords that permit access to the covered account.
- Close existing covered account and reopen a new covered account.

Step 4: Administering the Program

Administering the program will consist of the following duties:

- Access to a copy of this program at all times through the Culver-Stockton College website.
- Staff training as necessary to effectively implement the program.
 - Training will consist of requirements of the Red Flags Rule, the policies and procedures that are set forth in this program, and the importance placed by the College on compliance with the program and the prevention and mitigation of identity theft.
- Overseeing 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 flags rules and validated by appropriate due diligence may be considered to be meeting these requirements
 - Only information that is required by the service providers to conduct their duties will be shared by the College. Culver-Stockton College will collect and maintain all service providers' (who collect personal information of students, employees, and alumni) documents confirming their compliance with the "Red Flags Rule".
- Periodic Updates
 - This program will be reviewed, updated, and reapproved to reflect any changes in risks of identity theft. These changes in risks can consists of the College's experience with identity theft, changes in means of occurrence of identity theft, changes is methods of preventing and detecting identity theft, and changes in the way relationships are structured between the College and other entities (students, faculty, staff, service providers, etc.)

For additional information on the Federal Trade Commission's Red Flags Rule, please visit the following website: <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>