Curry College's Red Flag Identity Theft Prevention Program

The Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act), that is intended to reduce the risk of identity theft. This policy is intended to detect, prevent, and mitigate opportunities for identity theft at Curry College. The Red Flag Rule applies to Curry due to our participation in the Perkins Loan program. We have determined that there is a low risk of identity theft at Curry College.

Existing Policies and Procedures

Most offices at Curry College maintain information in both electronic and paper files, which may contain biographical, academic, health, and/or financial records. These records may also include student billing information including Federal Perkins Loan records. Policies to insure compliance with Gramm-Leach-Bliley Act (GLB), Family Educational Rights and Privacy Act (FERPA), and Payment Card Industry security standards (PCI), system and application security, and internal control procedures provide an environment where identify theft opportunities are mitigated. Records are safeguarded to ensure the privacy and confidentially of student, parents, alumni and employees.

The Office of Human Resources performs credit and criminal background checks on some potential employees prior to their date of hire. Criminal background checks are performed on any staff member who has unsupervised access to residence halls, and criminal background checks and credit checks are performed on employees whose positions require them to have regular access to cash, and/or who have computer access to payroll data. Access to this information is very limited and procedures to safeguard the data are in place.

- The student is required to give written authorization to the Registrar's Office if their non-directory information is permitted to be shared with another party. A FERPA disclosure statement is available to students informing them of their rights under FERPA. The student is given the opportunity to provide billing addresses for third party billing (parents, companies, scholarship foundations, etc).
- Occasionally, the College will extend short term credit to a student for payment of their tuition bill which thus creates a covered account. The student signs a short term promissory note, which is stored in a secured area. If we receive information of an address change (which is a red flag), we verify the change by contacting the student before making the change in the administrative database system.
- Access to student data in Curry's Banner system is restricted to those employees of the College with a need to properly perform their duties.
- Social Security numbers are not used as identification numbers.
- All paper files are required to be maintained in locked filing cabinets or offices when not in use. All offices, when not occupied, are to be locked and in most cases alarmed.
- Access to employee data in Curry's ADP Human Resources and Payroll systems is restricted to only those employees of the College who need this access to properly perform their duties. Staff is requested to report all changes in name, address, telephone or marital status to the Human Resources Office as soon as possible; they are also requested to periodically verify those persons listed as contacts in case of an emergency, and those persons designated as beneficiaries to life and/or retirement policies.
- The College is sensitive to the personal data (unlisted phone numbers, dates of birth, etc.) that it maintains in its personnel files and databases. We do not disclose

personal information, except by written request or signed permission of the employee unless there is a legitimate business "need-to-know", or if compelled by law.

- Every effort is made to limit the access to private information to those employees on campus with a legitimate "need-to-know. Staff who have approved access to the administrative information 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 the College.
- The College's official personnel files for all employees are retained in the Human Resources Office. Employees have the right to review the materials contained in their personnel file.

Detecting Red Flag Activity

- Address discrepancies
- Presentation of suspicious documents
- Photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification
- Personal identifying information provided is not consistent with other personal identifying information on file with the University
- Documents provided for identification that appear to have been altered or forged
- Unusual or suspicious activity related to covered accounts
- Notification from students, borrowers, law enforcement, or service providers of unusual activity related to a covered account
- Notification from a credit bureau of fraudulent activity

Responding to Red Flags

- Should an employee identify a “red flag” (patterns, practices and specific activities that signal possible identify theft), they are instructed to bring it to the attention of the Registrar or Director of Student Financial Services, or Director of Human Resources immediately. The administrator 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.

Oversight of Service Providers

- Curry College employs Affiliated Computing Services (ACS), a Federal Perkins Loan servicer for the purpose of billing and collection of Federal Perkins Loan payments. The only information that is shared with ACS is information required to properly bill and collect loan payment as established by the Department of Education. This includes student name, address, telephone number, social security number, and date of birth. Curry College will collect and maintain on file documents from ACS confirming their compliance with “Red Flag Rules”.
- Curry College employs Tuition Management Services (TMS), a tuition billing service, for monthly tuition payment plans. The only data that is shared with the TMS is information relating to the tuition payment plan established by the student or parent. Curry College provides the TMS with student id, Name prefix, name suffix,

last name, first name, mi, phone, street1, street2, street3, city, state, zip code, nation, email address, mother’s email address, father’s email address.

- Curry College will collect and maintain on file documents from TMS confirming their compliance with “Red Flag Rules”.

Periodic Update of Plan

This policy will be re-evaluated annually to determine whether all aspects of the program are up to date and applicable in the current business environments, and revised as necessary.

Operational responsibility of the program is delegated to the College’s Registrar and Director of Student Financial Services.