SOUTHEASTERN UNIVERSITY

GENERAL ADMINISTRATIVE POLICY

TITLE: Red Flag Rule Policy
POLICY NUMBER:
EFFECTIVE DATE: December 1, 2008
REVISION DATE: December 3, 2010
ACCREDITATION STANDARDS:

POLICY:

Minimize the risk of identity theft.

PURPOSE:

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 Southeastern University. The Red Flag Rule applies to Southeastern due to our participation in the Perkins Loan program, payment plans, our extension of credit for student accounts, and the fact that we request credit reports for some potential employees. Our analysis of the type and scope of activity covered in the regulation, and our risk assessment of potential identity theft opportunities has resulted in a determination that there is a low level risk of possible identity theft at Southeastern University.

SCOPE:

All persons associated with Southeastern University; or individuals participating in the:

- Federal Perkins Loan Program
- Southeastern payment plan (administered by third party)
- Credit reports in employee hiring process

DEFINITIONS:

"Identity Theft" - A fraud that is committed or attempted using a person's identifying information without authority.

"Covered Accounts" - Accounts that are used primarily for personal, family, household, or business purposes that involve or are designed to permit multiple payments or transactions; any account for which there is a reasonably foreseeable risk to members or the safety and soundness of Southeastern University. Covered Accounts include, but are not limited to, credit (debit) cards, loans, and student accounts.

FORMS AND APPLICABLE DOCUMENTS:

PROCEDURES:

Many offices at Southeastern University maintain files, both electronic and paper, of student biographical, academic, health, financial, and admission records. These records may also include student billing information, Perkins Loan records, and personal correspondence with students and parents. 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 identity 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. This population includes any staff member who has unsupervised access to residence halls, and 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.

- Parents may obtain non-directory information (e.g. grades, academic standing, etc.) at the discretion of the institution and after it is determined that the student is legally dependent on either parent. Staff who have access to HR and Payroll data have been versed on the policy of the University that non-directory information regarding employees is not being provided unless approved in writing by the employee.

- The student is required to give written authorization to the Office of the Registrar if their information is permitted to be shared with another party. A FERPA disclosure statement is sent out to students each year 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.).

- Occassionally, the University will extend short-term credit (through a payment plan) to a student for payment of their tuition bill which, thus, creates a covered account. This payment plan is administered by a third party. 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 Jenzabar system.

- Access to non-directory student data in the Jenzabar system is restricted to those employees of the University with a need to properly perform their duties. These employees are trained to know FERPA and "Red Flag" regulations.

- Social Security numbers are not used as identification numbers and these data are classified as non-directory student data.

- All paper files are required to be maintained in locked filing cabinets when not in use. All offices, when not occupied, are to be locked.

- Access to non-directory employee data in Southeastern's ADP Human Resources and Payroll systems is restricted to only those employees of the University who need this access to properly perform their duties. These employees are also trained to know FERPA and "Red Flag" regulations.

- Staff is required to report all changes in name, address, telephone, or marital status to the Human Resources Office as soon as posible; they also must 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 University is sensitive to the personal data (unlisted phone numbers, dates of birth, etc.) that it maintains in its personnel files and databases. We will not disclose personal information, except by written requrest or signed permission of the employee (for example, the Campus Directory), or 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 University.

- The University's official personnel files for all employees are retained in the Human Resources Office. Employees have the right to review the materials contains in their personnel file.

DETECTING RED FLAG ACTIVITY

- Address discrepancies
- Presentation of suspicious documents
- Photographs 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
- Unused 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 activites that signal possible identity theft), they are instructed to bring it to the attention of the University Registrar, Controller, 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

Southeastern University employs Campus Partners, a Perkins Loan servicer for the purpose of billing and collection of Perkins and Southeastern institutional loan payments. The only information that is shared with Campus Partners 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. Southeastern University will collect and maintain on file documents from Campus Partners confirming their compliance with “Red Flag Rules.”

Southeastern University uses two collection agencies for the purpose of collecting overdue student receivables and defaulted Perkins Loans. The only information that is shared with the collection agencies is that information required to perform credit checks, to perform address searches, and to properly bill and collect payment. This inclues student name, address, telephone number, social security number, and date of birth. Southeastern University will collect and maintain on file documents from all collection agencies regarding their compliance with “Red Flag Rules.”

Southeastern University employs Tuition Management Services (TMS), a tuition billing service, for monthly tuition payment plans. The only data that is shared with TMS is information relating to the tuition payment plan established by the student or parent. Southeastern University provides TMS with the student name, student Southeastern ID, and billing party name and address. Southeastern University 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 reponsibility of the program is delegated to the University Registrar and Direct of Student Financial Services.

APPROVAL:

DISTRIBUTION:

AUTHOR: