

University of the Southwest'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), to be implemented no later than August 1, 2009 that is intended to reduce the risk of identity theft. This policy is intended to detect, prevent, and mitigate opportunities for identity theft at University of the Southwest. The Red Flag Rule applies to USW due to the student's participation in Federal Loan programs, 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 University of the Southwest.

Scope of Covered Activities

- Payment plans and promissory notes for covered student accounts.
- Credit reports in employee hiring process

Existing Policies and Practices

Many offices at University of the Southwest maintain files, both electronic and paper, of student biographical, academic, health, financial, and admission records. These records may also include student billing information, federal 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 identify theft opportunities are mitigated. Records are safeguarded to ensure the privacy and confidentiality 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 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.) after the office responsible for the information has verified that either the student is legally a dependent of the parent or the student has completed a release form authorizing release of the information to the requesting 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 be provided unless approved in writing by the employee.

- The student is required to give written authorization to the Registrar's Office 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).
- University of the Southwest offers a Student Incentive Payment Plan (SIPP), a tuition billing service, an alternative payment method that enables students to remit their educational costs over four installments rather than the lump sum payment normally due one week before the start of classes. 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 CAMS system.
- Access to non-directory student data in USW's CAMS 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 containing personal information are kept in locked filing cabinets when not in use. All offices in which personal student or employee information are kept locked when not occupied.

- Access to non-directory employee and student data 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 requested to report all changes in name, address, telephone or marital status to the Human Resources Office as soon as possible; 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.
- Students are requested to report all changes in status including name and address changes.

- The University is sensitive to the personal data (unlisted phone numbers, dates of birth, etc.) that it maintains in its personnel files and student databases. We will not disclose personal information, except by written request or signed permission of the employee or student (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 student information database 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 contained in their personnel file.
- The Office of Enrollment Services begins at the application stage to ensure the identity of applicant. This is done through requiring students indicate a social security number and mother's maiden name and to submit a picture accompanied by government issued identification.
- International student applicants who do not have social security numbers are required to enter 5 digits and the year of their birth as a substitute for a social security number.
- Application data is encrypted as it is transmitted from the web site to the Office of Enrollment Management.
- The University's official student records are retained in the Office of the Registrar. Students have access to records by written request from the Office of the Registrar and as made available in the eStudent Portal.
- The Office of Financial Aid confirms student identity by requiring either the student ID or social security number on all written requests regarding financial aid. If the student's personal information is being requested by the student over the phone or in person, financial aid staff will ask the student to provide student ID, social security number, and/or date of birth before information is released. If the Office of Financial Aid staff has any concern regarding the identity of the student, no information will be released.
- The Office of Housing and Security compares all information received on housing applications and refund requests with the official student record on CAMS. Should a discrepancy be found, additional identifying information is requested from the student. The student is referred to the Office of the Registrar for records to be updated.
- Each student is given individual login and password to access academic and financial records through their eStudent portal.

Detecting Red Flag Activity

- Address discrepancies
- Social Security Number discrepancies
- Presentation of incomplete or 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 attempt to verify the information received. If the "red flag" cannot be resolved, they are instructed to bring it to the attention of the Dean, director or Senior Administrator. Upon verification, the University Registrar or Director of Human Resources is immediately contacted. The Registrar or Director of Human Resources will investigate the threat of identity theft to determine if there has been a breach and will communicate the threat to the CFO or Provost to respond appropriately to prevent future identity theft breaches. The CFO or Provost will determine if additional actions are warranted which may include notifying and cooperating with appropriate law enforcement and notifying the student or employee of the attempted fraud.

Oversight of Service Providers

- University of the Southwest uses Immediate Credit Recovery Inc. for the purpose of collecting overdue student receivables. 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 includes a copy of the billing statement, student name, address, telephone number, social security number, and date of birth. University of the Southwest will collect and maintain on file documents from all collection agencies regarding their compliance with "Red Flag Rules".
- USW has received verification from the New Mexico Educational Assistance Foundation (NMEAF) and the New Mexico Student Loan Guarantee Corporation (NMSLGC) that these entities have established Red Flag Rules and Procedures.

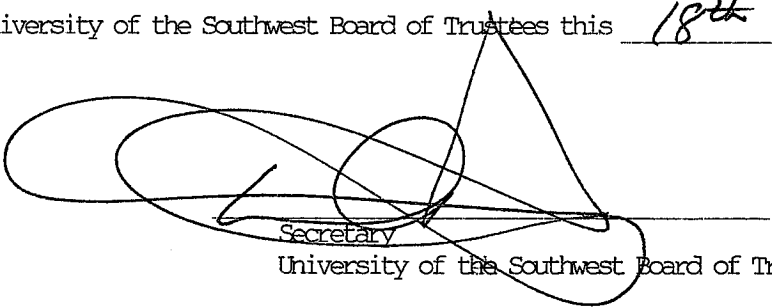
- USW uses Texas Guarantor (TG) which has Fraud alert and identity theft resources posted on their web site, http://www.tgslc.org/resources/dataprivacy/dataprivacy_fraudalert.cfm.
- USW uses ELM Resources (Education Loan Management). ELM Confidentiality / Security policies are posted at <http://www.elmresources.com/web/guest/privacypolicy>.

Periodic Update of Plan

This policy will be re-evaluated annually by a committee representing the Business Office, Office of Financial aid, Office of the Registrar, Office of Enrollment Management and Office of Technology Services 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 University Registrar and Director of Technology Services.

Adopted by the University of the Southwest Board of Trustees this 18th day of June, 2009.


Secretary
University of the Southwest Board of Trustees