Williams Baptist College
IDENTITY THEFT POLICY/PROGRAM

Summary

Williams Baptist College (the “College”) has developed this identity theft program (the “Program”) pursuant to the Federal Trade Commission’s Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Policy/Program was developed by the Vice President for Finance.

Purpose

The Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program established procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flag that has been detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions (As Defined in the Act)

A. “Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”

B. “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

C. “Covered Account” means (i) an account that a creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions or (ii) an account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

D. “Program Administrator” is the individual designated with primary responsibility for oversight of the Program.

E. “Identifying Information” is “any name or number that may be used alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license
or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code.

Identified Accounts

The College has identified the following covered accounts:

1. Plus Loans (Williams is a direct lender; collection is performed by the U. S. Government)
2. Stafford Loans (Williams is a direct lender; collection is performed by the U. S. Government)
3. Perkins Loans
4. Alternative Loans
5. Deferred Tuition Payments
6. Student Accounts

Risk Assessment

For the College administered covered accounts listed above, the existing risk is that a fraudulent request is made for a refund on an overpaid account resulting from a loan and/or direct payment. Since the College is solely responsible for issuing refunds on these accounts, the risk resides at the College level.

Control Procedures

As noted above, the primary risk associated with the covered accounts relates to refunds on student accounts and loan accounts. The following control procedures mitigate this risk:

Refund Checks
All credit refund checks except Plus Loans are placed in on-campus student mail boxes or mailed to their official permanent address. Credit checks from Plus Loans are mailed to official permanent addresses.

Account Statements
All student account statements are placed in student mail boxes and/or mailed to their official permanent address.

Address Changes
Changes to mail boxes or official permanent addresses may only be made in person at the post office (for on-campus boxes) or in the registrar office (for a change in the official address). Changes must be made by the student and may require a valid identification card. A change in name requires the appropriate legal document subject to the specific instance, such as a
marriage certificate. The registrar office will notify all administrative office of changes to a student official address.

**Release of Identifying Information**
No administrative office is to release identifying information to any individual without prior positive proof of identification. This includes but is not limited to a driver’s license, WBC identification card, or valid passport.

**Access to information**
All hardcopy data is to be kept in a secure area at all times. When possible, data will be kept under lock and key in areas not accessible to non-office personnel. After hours all information is kept in areas inaccessible to non-authorized personnel.

All electronic data is to be password protected and physical access to terminals is restricted.

**Red Flags**

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag is apparent, it should be investigated.

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request to mail something to an address not listed on file; and
4. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

**Response to Red Flags**

The program provides appropriate responses to detect red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the Red Flag;
2. Contact the student or employee;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.
Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the College’s Vice President for Finance. The Vice President for Finance is responsible for program administration, ensuring appropriate training of the College’s staff on the Program, reviewing any staff reports regarding the detection of red flags on the identified covered accounts and the steps for preventing and mitigating Identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

Updating the Program

This Program will be periodically reviewed and updated to reflect changes in risks to students and employees and the soundness of the College from identity theft related to the noted covered accounts. At least once per fiscal year, the Vice President for Finance will consider the College’s experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College’s business arrangements with other entities, as they relate to this program. After considering these factors, the Vice President for Finance will determine whether changes to the Program, including the listing of red flags, are warranted. If warranted, the Program will be updated.

Staff Training

College staff responsible for implementing the Program shall be trained either by or under the direction of the Vice President for Finance in the detection of red flags, and the responsive steps to be taken when a Red Flag is detected.

Updated 1-1-2011