Rosedale Bible College

Identity Theft Prevention Policy
(Red Flags Rule)

I. PROGRAM INTRODUCTION

Rosedale Bible College (“College”) developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”). The rule requires “financial institutions” and “creditors” holding “covered accounts” to develop and implement a written identity theft prevention program designed to identify, detect and respond to “Red Flags.”

II. RED FLAGS RULE DEFINITIONS

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

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

A “**Covered Account**” is an account used primarily for personal, family, household or business purposes that involves or is designed to permit multiple payments or transactions; any account for which there is a reasonably foreseeable risk from identity theft to customers.

A “**Creditor**” is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit.

“**Program Administrator**” is the individual designated with primary responsibility for oversight of the program. See Section VII below.

“**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, or student identification number.

III. RED FLAGS RULE REQUIREMENTS

Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operations. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts 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 Flags that are detected to prevent and mitigate identity theft; and

4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from identity theft.

IV. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft.

The College has conducted an assessment of the risk of identity theft for its students. Most student accounts are paid at the beginning of a semester or term and, therefore, do not fall under the definition of a Covered Account. For those students who opt to pay for tuition and fees under the payment plan, the risk of identity theft is very low because College personnel know the students personally, the student must appear on campus to attend classes, the College has never experienced an incident of identity theft, and identity theft is not common in this context.

The College identifies the following Red Flags in each of the listed categories:

A. Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information;
4. Application that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person failing to provide complete personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the student.

C. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the College that a student is not receiving mail sent by the College;
6. Notice to the College that an account has unauthorized activity;
7. Breach in the College's computer system security; and
8. Unauthorized access to or use of student account information.

D. Alerts from Others

Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in identity theft.

V. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via fax, or via email); and
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes;

VI. PREVENTING AND MITIGATING IDENTITY THEFT

A. Prevention

In order to prevent the likelihood of identity theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Protect access to all College computers with secure passwords;
2. Update computer operating systems and applications and virus protection on a regular basis;
3. Ensure that access to Covered Accounts is limited to authorized personnel and protected by passwords;
4. Report any unauthorized access to or breach of a Covered Account immediately to the Program Administrator;
5. Avoid the use of social security numbers where they are not needed.

B. Mitigation

In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Notify the Program Administrator for determination of the appropriate step(s) to take;
2. Contact the student or applicant;
3. Continue to monitor a Covered Account for evidence of identity theft;
4. Change any passwords that permit access to Covered Accounts;
5. Opt not to open a new Covered Account;
6. Close an existing Covered Account;
7. File or assist in filing a Suspicious Activities Report ("SAR");
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator who may be the Business Manager or the position responsible for Risk Management. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags 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.

B. Staff Training and Reports

College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of the College's failure to comply with this Program. Periodically, College staff responsible for implementation and administration of the Program shall report to the Program Administrator on compliance with this Program.

C. Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship.

D. Program Updates

The Program Administrator will periodically review and update this Program to reflect changes in risks to students and the soundness of the College from identity theft. In doing so, the Program Administrator will consider the College's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program will be updated.