Red Flag Identity Theft Prevention
Date of original implementation: 01/2016
Date of Last Revision: 05/2016

Summary
Success Education Colleges ("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.

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 establishes 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 Team Members 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

A *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.

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, individual identification number, computer's Internet Protocol address, or routing code.

Identity Theft means 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.

College Covered Accounts
The College has identified the following covered accounts:

College administered covered accounts - Students:

1. Plus Loans (The College participates in the Federal Student Aid Direct Loan Program)
2. Stafford Loans (The College participates in the Federal Student Aid Direct Loan Program)
3. Perkins Loans — (Serviced by UNISA)
4. Tuition Payment Plans
5. Student Accounts

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

A. Suspicious Documents Red Flags
   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) Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information Red Flags
   1) Identifying information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);
   2) Identifying information presented that is inconsistent with other sources of information and which raises suspicion of identity theft (example: inconsistent undergraduate institutions during the same time period);
   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 known to have been given by another individual;
6) An address or phone number presented that is the same as that of another person who is not a family member, roommate or other documented relation;
7) A person fails to provide complete personal identifying information on an application when reminded to do so; and

C. Suspicious Covered Account Activity or Unusual Use of Account Red Flags
1) Change of address for an account followed by a request to change the individual's name;
2) Mail sent to the individual is repeatedly returned as undeliverable;
3) Notice to The College that an account has unauthorized activity;
4) Breach in The College's computer system security; and
5) Unauthorized access to or use of individual account information.

D. Alerts from Others Red Flag: Notice to The College from an individual, 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.

Detecting Red Flags

Initial Enrollment – In order to detect Red Flags identified above associated with the enrollment of an individual, Team Members will take the following steps to obtain and verify the identity of the person opening the account:
a. Require certain identifying information such as name, previous academic records, home address, or other identification; and
b. Verify the individual's identity at the time of issuance of their individual identification card (review of driver's license or other government issued photo identification).

Existing Accounts – In order to detect Red Flags identified above for an existing Covered Account, Team Members will take the following steps to monitor transactions on an account:
a. Verify, in person, the identification of the individual requesting information related to student records, personal information, and financial and banking information;
b. Verify the validity of any request to change or add a new address submitted by email and provide the individual a reasonable means to promptly report incorrect billing address changes.

Consumer ("Credit") Report Requests – In order to detect any of the Red Flags identified above for an extension of credit for which a credit or background report is sought, Team Members will take the following steps to assist in identifying address discrepancies:
a. Require written verification from the applicant that the address provided by the applicant has been accurately provided to the consumer reporting agency; and

b. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that The College has reasonably confirmed is accurate.

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:

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

Control Procedures

Protect Individual Identifying Information. The College will also take steps to further 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 individual identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure; ensure computer virus protection is up-to-date; and, ensure that office computers with access to Covered Account information are password protected;
2. Ensure complete and secure destruction of paper documents and computer files containing individual account information when a decision has been made to no longer maintain such information;
3. Avoid use of social security numbers (use The College's assigned student ID number); and
4. Require and keep only the types of individual information that are necessary for The College.

Service Providers – The College will take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more Covered Accounts. However, the processes transacted by these providers represent funds owed to the College, mitigating the risk of theft to the account holders. Additionally, The College will take steps to ensure the existence of adequate Red Flag policies and procedures enacted by these providers.

Risk Associated With The Covered Accounts Related To Refunds On Student Accounts And Loan Accounts – The following control procedures mitigate this risk:

1. Refunds due to overpayments will be administered only by the Financial Aid/Fiscal Office. All inquiries are directed only to this office.
2. Checks are paid and mailed to the official name and address within the College's student database management system or may be picked up in person. The student must provide his/her valid state-issued identification, a current US driver's license, or valid passport when receiving the check in person. A student may not request a specific payee or address that is different from the information in the College's student database management system.
3. Students must make any permanent name or address change in person at the Registrar's Office. A change in name requires the appropriate legal document subject to the specific instance, such as a marriage certificate. An address change requires official proof such as a utility bill, rental lease, mortgage, or other appropriate documentation. These changes must be updated in The College's student database management system before requesting the refund.

Oversight of the Program

Responsibility for developing, implementing, and updating this Program resides with the College's Chief Financial Officer (CFO). The CFO is responsible for program administration, ensuring appropriate training of the College's Team Members on the Program, reviewing any reports regarding the detection of red flags on the identified Covered Accounts, 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 the soundness of The College from identity theft related to the noted Covered Accounts. At least once per year, the CFO 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 that The College maintains, and changes in the College's business arrangements with other entities, as they relate to this program. After considering these factors, in consultation with the President, the CFO will determine whether changes to the Program, including the listing of red flags, are warranted.

Team Member Training

Team Members responsible for implementing the Program shall be trained either by or under the direction of the CFO in the detection of red flags, and the responsive steps to be taken when a Red Flag is detected.