I. PROGRAM ADOPTION

Golden Gate University ("University") 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. This Program was developed with the oversight of the Vice President, Academic Affairs and the approval of the University’s Board of Trustees.

In compliance with its legal obligations, the University has conducted an inquiry to determine whether it offers or maintains Covered Accounts, as that term is understood under the Rule, and, as a part of this inquiry, the University has conducted a risk assessment to determine whether it offers or maintains Covered Accounts, taking into consideration: the methods it provides to open its accounts; the methods it provides to access its accounts; and its previous experiences with Identity Theft.

Following this inquiry, the University has determined that it offers or maintains Covered Accounts. Accordingly, after consideration of the size of the University’s operations and account systems and the nature and scope of the University’s activities, and after review of the policies and procedures set forth in this Program, the Board of Trustees determined that the Program was appropriate for the University, and therefore approved this Program, effective May 1, 2009.

II. PURPOSE

The purpose of this Program is to combat Identity Theft in connection with new and existing Covered Accounts, and includes policies and procedures for detecting, preventing and mitigating Identity Theft, and enabling the University to:

1. Identify relevant Red Flags (defined below) for the Covered Accounts that the University offers or maintains;
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 from Identity Theft.
III. DEFINITIONS

Covered Account means:
1. 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; and
2. Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to persons that have a Covered Account or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

Creditor means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Identifying Information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person (e.g., name, address, telephone number, Social Security number, date of birth, government-issued driver’s license).

Identity Theft means a fraud committed or attempted using the Identifying Information of another person without authority.

Program Administrator is the person or persons charged by the University with the development, implementation, oversight, continued administration and updating of the Program. At the University, the Program Administrator is the Vice President, Academic Affairs. The Program Administrator may designate such senior management employee or employees as may be reasonably necessary or appropriate to assist in the duties of the Program Administrator.

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

IV. COVERED ACCOUNTS

The University has identified seven types of Covered Accounts, five of which are administered by the University and two of which are administered by a service provider:

University Covered Accounts:
1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, not involving PLUS loans
3. Direct student loans
4. Emergency loans
5. Book loans

Service provider Covered Accounts:
1. Deferred tuition payment plan administered by TMS. (See Section VIIIA.)
2. Perkins loans administered by ACS. (See Section VIIIB.)

V. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the University considers the types of Covered Accounts that it offers and maintains, the methods it provides to open its Covered Accounts, the methods it provides to access its Covered Accounts, and its previous experience with Identity Theft.

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

A. Suspicious Documents
   1. Identification document or card that appears to be altered or forged;
   2. Identification document or card on which a person’s photograph or physical description is not consistent with the appearance of the person presenting the document;
   3. An identification document or card that presents other information that is inconsistent with information provided by the student offering the document;
   4. An identification document or card that presents other information that is inconsistent with readily accessible information on file with the University; and
   5. An application that appears to have been altered or forged.

B. Suspicious Personal Identifying Information
   1. Identifying information presented that is inconsistent with readily accessible information on file with the University (example: inconsistent SSN, birth date);
   2. Identifying information presented that is inconsistent with other information the student provides;
   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 (example: an invalid phone number or fictitious billing address);
   5. Social Security number presented that is the same as one given by another person;
   6. An address or phone number presented that is the same as that of another person;
   7. A student fails to provide complete personal identifying information on an application when reminded to do so; and

C. Suspicious Covered Account Activity
   1. Nonpayment when there is no history of late or missed payments;
   2. A material change in account terms;
   3. A material change in account activity;
   4. Mail sent to the student is repeatedly returned as undeliverable;
   5. Notice to the University that a student is not receiving mail sent by the University;
   6. Notice to the University that an account has unauthorized activity;
D. Alerts from Others

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

VI. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new Covered Account, University 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, driver’s license, GGU student identity card or other identification;
2. Review the Identifying Information for authenticity;
3. Verify the individual’s identity from the Identifying Information; and
4. When appropriate, confirm the individual’s identity by reviewing College records or by directly contacting the student.

B. Existing Accounts

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

1. Verify the identity of the student if account service or information is requested (whether in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in account information given for billing and payment purposes.

VII. RESPONDING TO SUSPECTED IDENTITY THEFT

A. Prevent and Mitigate

In the event University 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. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Confirm the individual’s identity by reviewing University records or by directly contacting the student;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Decline to open a new Covered Account;
5. Close an existing Covered Account;
6. Provide the student with a new account number or student identification number;
7. Notify the Program Administrator for determination of the appropriate response;
8. Notify law enforcement;
9. Use professional judgment when determining that no response is warranted under the particular circumstances.

B. Protect Student Identifying Information

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

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to Covered Account information are password protected;
4. Avoid use of Social Security numbers;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of student information that are necessary for University purposes.

C. Report Identity Theft

In the event the University learns of possible Identity Theft, it will respond in the following manner:

1. The staff member who learns of the incident will notify his or her supervisor;
2. The staff member and the victim will write a brief description of what took place, citing transactions, dates, amounts and other information, and providing what documentation is available, and the staff member will forward this documentation to his or her supervisor;
3. The supervisor will notify the Program Administrator and will forward the documentation to the Program Administrator;
4. The Program Administrator or designee will offer support to the victim by providing information and literature assisting them him or her to contact creditors, credit bureaus, and other persons or entities, as necessary;
5. The Program Administrator or designee will file a police report, if necessary.

VIII. Service Provider Covered Accounts

A. Tuition Payment Plans

The University tuition payment plan requires recurring payments on a student’s account using a third party vendor, Tuition Management Systems (TMS). This payment plan has been reviewed and the potential for risk in this area is deemed minimal.
B. Perkins Loan

Name changes and address changes are typically made on line by the borrower through an authentication process with the University’s current billing service provider, Affiliated Computer Services, Inc. (ACS). ACS provides the College with a Basic Red Flag Regulation Service for a nominal fee that includes the tagging of all suspicious activity (e.g., multiple address changes, attempts to get information by calling into their office, etc.) and producing a monthly report. If the Perkins Loan Coordinator were to receive a name and/or address change, she/he would require valid photo identification and supporting documentation (e.g., utility bill, marriage certificate, etc.), before updating the ACS system.

IX. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator, who shall keep the Office of the President reasonably advised regarding the Program and instances of Identity Theft pertaining to students, faculty, staff or the University. The Program Administrator will be responsible for: (1) ensuring appropriate training of University staff to effectively implement the Program; (2) reviewing staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft; (3) determining which steps of prevention and mitigation should be taken in particular circumstances; and (4) considering periodic changes to the Program.

B. Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of and response to Red Flags. University employees are expected to notify the Program Administrator once they become aware of an incident of suspected Identity Theft or of the University’s failure to comply with this Program.

At least annually, or as otherwise requested by the Program Administrator, University staff responsible for implementing the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents of Identity Theft and the University’s response, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University 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 University's Program and
report any Red Flags to the Program Administrator or designee.

D. Program Updates

The Program Administrator or designee will periodically review and update this Program to reflect changes in risks to students and the soundness of the University from Identity Theft based on factors such as: the University’s experiences with Identity Theft; changes in Identity Theft methods; changes in Identity Theft detection and prevention methods; and changes in the University’s business arrangements with other entities.