Identity Theft Prevention Program

Effective: November 1, 2009

I. BACKGROUND

Galveston College ("College" / "Institution") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule

b. Address
c. Telephone number
d. Social Security Number
e. Date of birth
f. Government issued driver's license or identification number
g. Alien registration number
h. Government passport number
i. Unique identification number
j. Checking account information (used by customers making payments)
k. Computer's Internet protocol address, or routing code

4. Payroll Information – including but not limited to:
   a. Paychecks
   b. Pay stubs
   c. Bank account information (used by staff and faculty for direct deposit)
   d. Any other document or electronic file containing salary information

5. Credit Card Information – including but not limited to:
   a. Credit card number (in whole or in part)
   b. Credit card expiration date
   c. Cardholder name
   d. Cardholder address

6. Medical Information – including but not limited to:
   a. Doctor names and claims
   b. Insurance claims
   c. Prescriptions
   d. Any related personal medical information

7. Covered Account – a College account that is an individual service account held by customers of the College whether residential, commercial, or industrial.
   a. Any account the College offers or maintains primarily for personal, family, or household purposes, that involves multiple payments or transaction; and
   b. Any other account the College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College from Identity Theft.

III. PROGRAM ADMINISTRATION; TRAINING, REPORTING

The Director of Human Resources and Risk Management or designee by the College President (hereinafter, the "Program Administrator") is responsible for overall Program management and administration. The Program Administrator shall provide appropriate identity theft training for relevant College faculty and staff and provide reports and

periodic updates to the Vice President for Administration and the Board of Regents on at least an annual basis.

The Identity Theft Prevention Board Policy (C Local) and this Program shall be posted on the College's main website, as well as departmental web pages including but not limited to the Registrar's Office, Financial Aid, the Business Office, and Human Resources / Risk Management. Periodic email notifications of this policy, no less than once a year shall be sent to students, faculty and employee of the College.

The annual report shall identify and evaluate issues such as the effectiveness of the College's policies and procedures for addressing the risk of identity theft with respect to Covered Accounts, oversight of service providers (third party contractors), significant incidents involving Identity Theft and the College's response, and any recommendations for material changes to the Board Policy or the Program. As part of the annual review, Red Flags may be revised, replaced, or eliminated. Defining new Red Flags may also be appropriate.

IV. RISK MANAGEMENT

A. The College may incorporate relevant Red Flags from sources such as:
   1. Incidents of identity theft that have been experienced at the College or by other institutions of higher education.
   2. Methods of identity theft identified by the College or other Creditors that reflect changes in identity theft risks.
   3. Applicable supervisory guidance.

B. The College may include relevant Red Flags from the following categories, if deemed appropriate:
   1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
   2. The presentation of suspicious documents
   3. The presentation of suspicious personal identifying information, such as a suspicious address change.
   4. The unusual use of, or other suspicious activity related to a Covered Account.
   5. Notices from customers, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts.

Administrator so that up-to-date knowledge of the ERP system protection methods are verified and documented.

B.

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. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer 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 credit report);
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 inconsistent 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 customer;
6. An address or phone number presented that is the same as that of another person;

Red Flag

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

VII.

2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

F. **Protect customer identifying information**

In order to further prevent the likelihood of identity theft occurring with respect to College accounts, the College will take the following steps with respect to its internal operating procedures to protect customer 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 customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and require and keep only the kinds of customer information that are necessary for College purposes.