Galveston College

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 (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed in concert with Galveston College Policy CS (LOCAL) – Identity Theft Prevention, approved by the Galveston College Board of Regents (“Board”) on October 14, 2009. After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, Management has determined that this Program was appropriate for Galveston College. The program (by federal mandate) becomes effective November 1, 2009.

II. PROGRAM PURPOSE, SCOPE & DEFINITIONS

A. Purpose

The purpose of the Identity Theft Protection Program is three-fold:

1. To ensure the security and confidentiality of Customer/Consumer identifying information including that of students, faculty and employees of the College.
2. To prevent unauthorized access, theft, and/or disclosure of Customer/Consumer identifying information stored in the College’s ERP system, departmental file cabinets, or that has been provided to 3rd parties.
3. To detect any unauthorized intrusion, theft, and/or disclosure of Customer/Consumer identifying information that has been collected by the College.

B. Scope

This program applies to all employees, faculty, staff, temporary workers, and other workers at the College contractors, as well as consultants, and third parties that have received personal information from the College.

C. Definitions of terms

The following are terms and definitions relating to the subject of identity theft:

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

2. Identity Theft – fraud committed using the identifying information of another person.

3. Identifying Information – including but not limited to:
   a. Name (including maiden name)

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 (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 (CS 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.

V. PREVENTIVE / PROTECTIVE ACTIONS TO BE TAKEN

The following actions will be taken to protect and defend Customer/Consumer identifying information from unauthorized access, theft, and/or disclosure:

A. The College's ERP system will be protected from external intrusion (hacking) by installing adequate, up to date software for this purpose (and from unauthorized internal access) and by promoting and enforcing effective security hierarchies, including password protocols. An annual departmental survey will be conducted by the Program

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

B. Departmental files containing hard copies of Customer/Consumer identifying information will be identified and reported to the Program Administrator. File cabinets are to be kept locked when not in use. Monitoring and controlling access of these files will be the responsibility of the department supervisor. An annual departmental survey will be conducted by the Program Administrator so that up-to-date knowledge of the location of all stored confidential information is verified and documented.

C. Printed documents that have been identified as trash, but which contain Customer/Consumer identifying information will be placed in a locked bin for future shredding or immediately shredded using a mechanical crosscut.

D. An annual survey will be conducted by the Program Administrator to confirm that all 3rd party entities, to which College staff has forwarded identifying information, do maintain an FTC-approved Identity Theft Prevention Program, to safeguard the information. Once confirmed, a copy of each 3rd party entity's program will be collected and stored in the College's Identity Theft Prevention Program manual.

E. A valid photo ID will be required any time identifying information related to a Covered Account is collected or changed. This includes but is not limited to payments received using a credit or debit card, information collected for financial aid, information collected for registration / admission, and information collected for background checks, drug tests, communicable diseases or proof of vaccination (bacterial meningitis vaccine for athletes).

VI. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the 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. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. 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. 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 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 customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. A person’s identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder'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 (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the College that a customer 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 customer account information.

E. Alerts from Others

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. DETECTING RED FLAGS.

A. New Accounts

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

B. Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

C. Existing Accounts

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

D. Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

VIII. PREVENTING AND MITIGATING IDENTITY THEFT

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:

E. Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;

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.