Category: Operations

Policy Title: Identity Theft Prevention - Red Flag Rules

Policy Statement: The Board of Trustees requires college staff to establish policies and procedures to combat identify theft. Procedures are developed and implemented to detect, prevent, and mitigate identify theft in connection with new and existing accounts.

Procedures:

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration jointly issued regulations pursuant to the Fair and Accurate Credit Transactions Act ("FACT") known as the "Red Flag Rules." Garden City Community College recognizes that some of its activities are subject to the provisions of the FACT Act and its Red Flag Rules. Additional information can be found at: http://www.ftc.gov/redflagsrule

GCCC adopts these procedures to identify relevant Red Flags for new and existing covered accounts and incorporate said Red Flags into the program; detect Red Flags that have been incorporated into the program; respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and ensure the program is updated periodically to reflect changes in risks to students, employees or contractors or to the safety and soundness of the individual from identity theft.

Approval and Management; Program Administration; Training; Annual Report

The Chief Financial Officer (hereinafter, the Program Administrator) is responsible for overall program management and administration. The Program Administrator shall provide appropriate identity theft training for selected college employees and provide reports and periodic updates to college administration on an annual basis.

The annual report shall identify and evaluate issues such as the effectiveness of the college's procedures for addressing the risk of identity theft with respect to Covered Accounts, oversight of service providers, significant incidents involving identity theft and the college's response, and any recommendations for material changes to this Program.

Definitions

1. A "Creditor" is any entity that regularly extends, renews, or continues credit or regularly arranges for the extension, renewal or continuation of credit.
2. A "Covered Account" is a consumer account designed to permit multiple payments or transactions and any other account for which there is a reasonably foreseeable risk from identity theft.
3. A "Customer" is a person with a Covered Account at the college.
4. "Identity Theft" means fraud committed or attempted using the identifying information of another person.
5. "Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.
6. "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, but not limited to: 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, student identification number, computer's Internet Protocol address or routing code.

Applicability

This program applies to all staff, faculty, students and all personnel affiliated with third parties providing services to the college relating to Covered Accounts and/or Sensitive Information within the custody of control of the college.

Sensitive Information to be Protected

1. Personal Information upon enrollment, hire or contract
    - Social Security Number
    - Date of Birth
    - Address
    - Phone Numbers
    - Maiden Name

2. Payroll Information
    - Paychecks
    - Paystubs
    - Any document or electronic file containing payroll information

3. Medical Information for employee or student
    - Doctor names and claims
    - Insurance claims
    - Any personal medical information

4. Credit Card Information
    - Credit card number (in part or whole)
    - Credit card expiration date
    - Cardholder name
    - Cardholder address

Risk Assessment

1. GCCC will consider the following risk factors in identifying Red Flags for Covered Accounts, if appropriate:
    a. The types of Covered Accounts offered or maintained;
    b. The methods provided to open Covered Accounts;
    c. The methods provided to access Covered Accounts; and
    d. Past experience with identity theft.

2. GCCC, on a periodic basis, will incorporate relevant Red Flags from sources such as:
    a. Incidents of identity theft that have been experienced or that have been experienced by other colleges and universities;
    b. Methods of identity theft known by us or other Creditors that reflect changes in identity theft risks; and,
    c. Applicable supervisory guidance.

3. GCCC identifies the following Red Flags in each of the following categories:
    a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
    b. The presentation of suspicious documents;
    c. The presentation of suspicious personal identifying information, such as a suspicious address change;
    d. The unusual use of, or other suspicious activity related to a Covered Account; and,
    e. Notices from customers, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts.

4. The following instances are examples of Red Flags recognized by the college:

    A. <u>Notifications or warnings from a consumer reporting agency</u>
        1. A fraud or active duty alert is included with a consumer report;
        2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
        3. A consumer reporting agency provides a notice of address discrepancy that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer;
        4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
            a. A recent and significant increase in the volume of inquiries;
            b. An unusual number of recently established credit relations;
            c. A material change in the use of credit, especially with respect to recently established credit relationships; or,
            d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or Creditor.

    B. <u>Suspicious Documents</u>
        1. Documents provided for identification appear to have been altered for forged;
        2. The photo or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
        3. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or customer presenting the identification; and,
        4. Other information of the identification is not consistent with readily accessible information that is on file with the college.

    C. <u>Suspicious Personal Identifying Information</u>
        1. Personal Identifying information provided is inconsistent when compared against external information sources. For example:
            a. The address does not match any address in the consumer report; or,
            b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

2. Personal identifying information is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the Social Security Number range and date of birth.
3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources utilized by the college, such as:
    a. The address on an application is the same address provided on a fraudulent application; or,
    b. The telephone number on an application is the same as the phone number provided on a fraudulent application.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal third-party sources used by the college, such as:
    a. The address on an application is fictitious, a PO box, or a prison; or,
    b. The telephone number is invalid, or is associated with a pager or answering device.
5. The Social Security Number provided is the same as that submitted by other persons.
6. The address or phone number provided is the same as that submitted by others.
7. The person who has a covered account fails to provide all required identifying information.
8. Personal identifying information provided is not consistent with personal identifying information that is on file at the college.

D. <u>Unusual use of, or Suspicious Activity Related to the Covered Account</u>
    1. A new Covered Account is used in a manner commonly associated with known patterns of fraud, such as the customer failing to make first payment of the payment plan and no subsequent payments.
    2. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
    3. The college is notified that the customer is not receiving paper account statements.
    4. The college is notified of unauthorized charges or transactions in connection with a customer's Covered Account.
    5. The college is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the college may have an open account for a person engaged in identity theft.

<u>Protective Actions to be Taken</u>

1. File cabinets, desk drawers, storage cabinets and any other space containing documents with Sensitive Information will be locked or otherwise secured when not in use at the end of each workday or when unsupervised.
2. Writing tablets, note pads, post-its, etc. in common shared work areas will be erased, removed, or shredded when not in use.
3. Passwords for the college database will not be shared.
4. Keys will not be given to persons other than to those for whom the key request is made.
5. Sensitive Information to be discarded will be placed in a locked shred bin or immediately shredded using a mechanical cross cut shredding machine.
6. A photo ID will be required any time a request is made in person to change information to a Covered Account.

7. A photo ID will be required for picking up any check of any origin, such as payroll, loan, refund, etc., from the Business Office or the Payroll Office.

Detection of Red Flags

GCCC shall address the detection of Red Flags in connection with the opening of Covered Accounts by

1. Obtaining identifying information about and verifying the identity of newly hired employees, newly enrolled students, etc. Identifying information may include name, date of birth, residential or business address, principal place of business for an entity, SSN, driver's license or other identification;
2. Verifying identity, such as by reviewing a driver's license or other identification.
3. Monitoring transactions through photo ID verification.
4. Requiring transactions through photo ID verification.
5. Rejecting any application for a service or transaction that appears to have been altered or forged.
6. Verifying identity via a consumer reporting agency which will independently contact the newly hired employee, newly enrolled student as appropriate for admission to selected programs, etc.

GCCC shall address the detection of Red Flags in connection with existing Covered Accounts by:

1. Verifying identity if an employee, student or contractor requests information (in person, via telephone, via facsimile, via email).
2. Verifying the validity of requests to change mailing addresses.
3. Not sharing identity information with anyone, including the employee, student or contractor. Requiring them to give the information and verify with the information on the account.
4. Verifying changes in banking or credit card information given for billing and payment purposes.

Response to Red Flags

GCCC shall respond quickly to prevent identity theft. In all cases Red Flags are to be reported to the Chief Financial Officer. Response to Red Flags may include, but not be limited to:

1. Contacting owner of account in question by:
    a. Electronic method (e.g. email, text message, etc.)
    b. Written letter via the USPS
    c. Phone number on record
2. Terminating transaction
3. Changing any passwords, security codes, or other security devices that permits access to a Covered Account
4. Reopening a Covered Account with a new account number
5. Not opening a new Covered Account
6. Closing an existing Covered Account
7. Notifying and cooperating with appropriate law enforcement
8. Continuing to monitor an Account for evidence of Identity Theft.
9. Determining that no response is warranted under the particular circumstances.

Oversight of Service Providers

The college will make reasonable efforts to ensure that the activity of a service provider engaged by the College to perform an activity in connection with Covered Accounts, is conducted with reasonable

policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The college shall request that a copy of the service providers Red Flag Policy be sent to the college for review and maintained on file.

Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be share with other College employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

Annual Updates

The administrators of the College shall annually review this policy and recommend revisions when necessary to address changes in risks to students, faculty and staff based upon factors such as:

1. Experiences with identity theft.
2. Changes in methods of identity theft.
3. Changes in methods to detect and prevent identity theft.
4. Changes in the types of accounts that the college offers or maintains.
5. Changes in organizational structure.

Program Administration

Training shall be conducted by the Program Administrator, Chief Financial Officer, for faculty and staff on an annual basis.

Additional information can be found at: http://www.ftc.gov/redflagsrule

Contacts: Chief Financial Officer

Approved Date: 5/1/2009

Policy History:

Keywords: identity, theft, protection, confidential,

Related Form: Click here to enter text.