IDENTITY THEFT DETECTION POLICY

SLT 6.9

Date of Last Update:
May 05, 2009

Approved By:

- Senior Leadership Team

Responsible Office:
Business and Finance

POLICY STATEMENT

Grand Valley State University (GVSU) will comply with the applicable requirements of 16 C.F.R. 681, a federal regulation issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003 requiring that financial institutions and creditors (which include higher education institutions) implement written programs that provide for the detection of and response to specific activities ("Red Flag") that could be related to identity theft.

Grand Valley State University is required to adopt policies and procedures to mitigate identity theft. Activities that cause GVSU to be considered a "creditor" under the Red Flags Rule include:

1. Participating in the Federal Perkins Loan program
2. Participating in alternative or private educational loans
3. Offering institutional loans to students, faculty, or staff.
4. Offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.
5. Stored Value Cards

PROCEDURES

Identification of Red Flags
In order to identify relevant Red Flags, GVSU considers the type of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experience with identity theft. GVSU identifies the following Red

Flags in each of the listed categories:

1. Notification and Warnings from Credit Reporting Agencies

a. Report of fraud accompanying a credit report
b. Notice or report from a credit agency of a credit freeze on an applicant
c. Notice or report from a credit agency of an active duty alert for an applicant
d. Receipt of a notice of address discrepancy in response to a credit report request
e. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity

2. Suspicious Documents

a. Identification document or card that appears to be forged, altered or inauthentic
b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
c. Other document with information that is not consistent with existing student information
d. Application for services that appears to have been altered or forged

3. Suspicious Personal Identifying Information

a. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates)
b. Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application)
c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
d. Identifying information presented that is consistent with fraudulent activity (example: an invalid phone number or fictitious billing address)
e. Social security number presented identical to one given by another student
f. Address or phone number presented that is the same as that of another person
g. A person fails to provide complete personal identifying information on an application when reminded to do so
h. A person's identifying information is not consistent with the information that is on file for the student

4. Suspicious Covered Account Activity or Unusual Use of Account

a. Change of address for an account followed by a request to change the student's name
b. Payments stop on an otherwise consistently up-to-date account

c. Account used in a way that is not consistent with prior use
d. Mail sent to the student is repeatedly returned as undeliverable
e. Notice to University that a student is not receiving mail sent by the University
f. Notice to GVSU that an account has unauthorized activity
g. Breach in GVSU's computer system security
h. Unauthorized access to or use of student account information

5. Alerts from Others

Notice to GVSU from a student, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft

Red Flag Detections

Student Enrollment

To detect any of the Red Flags identified above associated with the enrollment of a student, GVSU personnel 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, date of birth, academic records, home address or other identification
b. Verify the student's identity at time of issuance of student identification card (review driver's license or other government-issued photo identification)

Existing Accounts

To detect any of the Red Flags identified about for an existing covered account, GVSU personnel will take the following steps to monitor transactions on accounts:

a. Verify the identification of students if they request information (in person, via telephone, facsimile or email)
b. Verify the validity of requests to change billing address by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes
c. Verify changes in banking information given for billing and payment purposes

Consumer ("Credit") Report Requests

To detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, GVSU personnel will take the following steps to assist in identifying address discrepancies.

a. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report was made to consumer reporting agency

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 GVSU has reasonably confirmed is accurate

Preventing and Mitigating Identity Theft

In the event that GVSU 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:

a. Continue to monitor a covered account for evidence of identity theft
b. Contact the student or applicant for which the credit report was requested
c. Change any passwords or other security devices that permit access to covered accounts
d. Not open a new covered account
e. Provide the student with a new student identification number
f. Notify the Program Administrator for determination of the appropriate step(s) to take
g. Notify law enforcement
h. Determine that no response is warranted under the particular circumstances
i. Take appropriate steps to modify the applicable process to prevent similar activity in the future

Protecting Student Identifying Information

To further prevent the likelihood of identity theft occurring with respect to covered accounts, GVSU will take the following steps as they relate to internal operating procedures:

a. Ensure that the GVSU website is secure or provide clear notice that the website is not secure
b. 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
c. Ensure that office computers with access to covered account information are password protected.
d. Avoid use of social security numbers
e. Ensure computer virus protection is up to date
f. Require and keep only the kinds of student information that are necessary for GVSU purposes

Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (Committee) for GVSU. This Committee is headed by a Program

Administrator appointed by the President. Two or more individuals appointed by the Program Administrator comprise the remainder of the committee.

The Program Administrator is responsible for ensuring appropriate training of GVSU personnel review of staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identify theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

Staff Training and Reports

GVSU staff responsible for implementing the Program shall be trained either by, or under the direction of, the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. GVSU staff shall be trained, as necessary, to effectively implement the Program. GVSU employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of GVSU's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, GVSU staff responsible for development, implementation, and administration of 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, and significant incidents involving identity theft and management response, and recommendations for changes to the Program.

Service Provider Arrangements

When the GVSU engages a service provider to perform an activity in connection with one or more covered accounts, GVSU 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:

a. Require, by contract, that service providers have such policies and procedures in place
b. Require, by contract, that service providers review GVSU's Program and report any Red Flags to the Program Administrator or GVSU employee with primary oversight of the service provider relationship

Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students and soundness of GVSU's policies, procedures, protocols and practices from identity theft. In doing so, the Committee will consider GVSU's experience with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in GVSU's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the

Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program, subject to approval by the Senior Leadership Team.

DEFINITIONS

Account- a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purpose.

Account includes:

a. an extension of credit, such as the purchase of property or services involving a deferred payment; and

b. a deposit account

Card Issuer- a financial institution or creditor that issues a debit or credit card.

Consumer Reports- any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

a.Credit or insurance to be used primarily for personal, family, or household purposes;

b. Employment purposes; or

c. Any other purpose authorized under U.S. Code: Title 13k, 1681b

Covered Accounts- an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account. Any account that the financial institution or creditor offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation. This includes all student accounts or loans that are administered by GVSU.

Debit Card- any card issued by a financial institution to a consumer for use in initiating an electronic funds transfer from the account of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money.

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:

a. Name
b. Date of birth
c. Address
d. Government issued driver's license
e. Telephone number
f. Alien registration number
g. Social security number
h. Government passport number
i. Employer or taxpayer ID number
j. Student identification number
k. Computer Internet address
l. Routing code

Identity Theft- a fraud committed or attempted using the identifying information of another person without authority.

Program Administrator- the individual designated by the President with primary responsibility for oversight of the Program.

Red Flag- a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Service Provider- a person that provides a service directly to the financial institution or creditor.
