GRINNELL COLLEGE
IDENTITY THEFT DETECTION POLICY

SECTION 1: BACKGROUND

Identity theft is fraud committed or attempted using the identifying information of another person without authority. In response to the growing threat of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Public Law 108-159. This amendment to the Fair Credit Reporting Act charged the Federal Trade Commission with promulgating rules regarding identity theft. On November 7, 2007, the Federal Trade Commission promulgated the final rules, known as "Red Flag" rules, which have an effective date of November 1, 2008 and an enforcement date of May 1, 2009 for all non-banking institutions falling under these requirements.

The risk to the College from identity theft is of significant concern to the College and can be reduced only through the combined efforts of all employees whose job function relates to the administration of covered accounts.

Definitions and Scope

The rules apply to "financial institutions" and "creditors" with "covered accounts."

"Financial institution" is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a transaction account belonging to a consumer. Grinnell College is considered a financial institution due mainly to the various student loan programs and tuition payment plans in which it participates.

A "creditor" is defined as someone who regularly extends, renews, or continues credit, who regularly arranges for an extension, renewal, or continuation of credit, or who is an assignee of an original creditor. The College is considered a creditor with respect to its student loan programs and monthly tuition payment plans.

A "covered account" is 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." This policy incorporates this definition and charges the College with monitoring any such account for which there is a reasonably foreseeable risk of identity theft.

A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

A "customer" is anyone doing business on a regular basis with the college (i.e. students, parents, etc.)

SECTION 2: PURPOSE

The College adopts this identity theft policy to detect, prevent and mitigate identity theft in connection with the opening and accessing of covered accounts. The program will help the College:

1. Identify risks (i.e. red flags) that signify potentially fraudulent activity within new or existing covered accounts;

2. Detect red flags when they occur in covered accounts;

3. Respond to red flags to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and

4. Evolve with the current environment and or institutional changes to remain current in its efforts to prevent identity theft. In order to do this, the College will update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

SECTION 3: POLICY

3.A: Covered accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account for which there is a reasonably foreseeable risk of identity theft; or a reasonably foreseeable risk to the safety or soundness of the College from identity theft is covered by this program.

The College has the following covered accounts that are subject to these criteria:

- Student Loans including the Federal Perkins Loan, Federal Plus Loan and other institutional and donor loans.

- Monthly tuition payment plan account.

- Accounts credited and billed through the cashier's office including student accounts.

All faculty, staff and students have a card, referred to as a P-Card that they add money to for use at the bookstore, cafeteria, vending machines, and other locations on campus. This card is not used off campus. The risk of identity theft is low as the card holder's picture is on the front of the card, which is checked when the card is being used. All cards are non-transferable and are confiscated if the person using the card does not match the photo. As such, we do not consider these accounts to be a "covered account."

3.B: Red flags

3.B.1: Consumer Reports

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

- Alerts, notifications or warnings from a consumer reporting agency;
- A fraud or active duty alert included with a report from a consumer reporting agency;
- A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
- A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

- A recent and significant increase in the volume of inquiries;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

3.B.2: Suspicious documents

- Documents provided for identification that appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the College.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

3.B.3: Suspicious personal identifying information

Personal identifying information provided is inconsistent when compared against external information sources used by the College. For example:

- The address provided does not match any address in the report from a Consumer Reporting Agency;

- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or

- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College. For example, the address on an application is the same as the address provided on a fraudulent application.

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example:

    - The address on an application is fictitious, a mail drop; or

    - The phone number is invalid or is associated with a pager or answering service.

- The SSN provided is the same as that submitted by other persons opening an account or other customers.

- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers.

- The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

- Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

- When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

3.B.4: Unusual use of, or suspicious activity related to, the covered account

- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    - Nonpayment when there is no history of late or missed payments;
    - A material change in purchasing or usage patterns
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The College is notified that the customer is not receiving paper account statements.
- The College is notified of unauthorized charges or transactions in connection with a customer's covered account.
- The College receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the College
- The College is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

SECTION 4: RESPONDING TO RED FLAGS

4.A: Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the College from damages and loss.

- Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to your supervisor (i.e. department head).
- The department head will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

4.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

- Canceling the transaction;
- Notifying and cooperating with appropriate law enforcement;
- Notifying the Controller by sending a completed Red Flag Disclosure Form (Attachment II), so that the appropriate college officials are kept informed; and

- Notifying the actual customer that fraud has been attempted and detected.

SECTION 5: PERIODIC UPDATES TO PLAN

- At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

- Periodic reviews will include an assessment of which accounts are covered by the program.

- As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

- Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the College and its customers.

- The departments involved in administering any of the "covered account" will review and update their Red Flag Matrix, which outlines the applicable red flags for the department, how they arise, and the appropriate department response. See Attachment I for the Red Flag Matrices by Department.

SECTION 6: PROGRAM ADMINISTRATION

This policy provides for continued administration and oversight of the program, including:

- Approval of the initial written program by the Audit & Assessment Committee;
- Educate and work with the those departments whose responsibilities include administering covered accounts on the development, implementation, administration and oversight of the program;
- Staff training as necessary to effectively implement the program;
- Exercise of appropriate and effective oversight of service provider arrangements; and
- Completion of Red Flag by Department Matrices.

Each year in July the respective department heads will report to the Controller on compliance with the regulatory requirements for the prior fiscal year.

If significant issues, including incidents of identity theft are reported during the year, the Controller will discuss them with the Treasurer in order to determine if they warrant attention at the next Audit & Assessment Committee meeting.

6.A: Staff training

- Staff training shall be conducted for all employees for whom it is reasonably foreseeable that they may come into contact with covered accounts that may constitute a risk to the College or its customers.

- Service Providers will be provided this policy so that they are aware of the College's rules surrounding identity theft.

- The Department Heads are responsible for ensuring identity theft training for all requisite employees.

- Additional training will be provided if policy changes warrant such action.

6.B: Oversight of service provider arrangements

Service Providers used by the College including collection agencies, loan processors and deferred payment plan administrators are subject to these rules as they relate to the administration of covered account.

- It is the responsibility of the College to ensure that the activities of all Service Providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

- A Service Provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence (i.e. obtaining and carefully reading their policy), may be considered to be meeting these requirements.

- Any specific requirements should be specifically addressed in the appropriate contract arrangements.

Section 7: Policy Approval and Review

This policy will take effect immediately upon its passage by the Audit & Assessment Committee of the Board of Trustees on February 6, 2009. Reviewed and reaffirmed by the Grinnell College Audit & Assessment Committee of the Board of Trustees on April 28, 2017.

This policy will be reviewed every two years or as deemed necessary by the Treasurer's Office given a specific event or change in the college's environment. Any proposed changes to this policy will be submitted to the Audit & Assessment Committee of the Board of Trustees for approval.

Attachment I: Red Flag by Department Matrices
Attachment II: Red Flag Disclosure Statement

Note: Grinnell College leveraged the Model Identity Theft Policy and FACTA Compliance document prepared by Josh Jones, legal consultant for the University of Tennessee's MTAS (Municipal Technical Advisory Services). Grinnell received authorization for the use of this document from Michael Tallent, executive director of the University of Tennessee's MTAS.