BEREA COLLEGE Red Flag Rules/ Identity Theft Prevention Policy	Document No.	FIN002
	Effective Date	05/2009
	Revision Date	
	Pages	1-7
	Approval:	On File in F/A

Note: Action items are italicized

1.0 Background

On November 9, 2007, 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." For organizations that are subject to the Red Flag Rules, identity theft programs must be in place by May 1, 2009. The College recognizes that some of its activities are subject to the provisions of the FACT Act and its Red Flag Rules and hereby adopts this Policy and the following Identity Theft Prevention Program (the "Program").

2.0 Purpose

The purpose of the Red Flag Rules is to combat identity theft. Federal regulations require financial institutions and Creditors to implement a program to detect, prevent, and mitigate identity theft in connection with new and existing accounts.

3.0 Approval and Management; Program Administration; Training; Annual Report

The Controller or such other person that may be appointed from time to time by the President of the College (hereinafter, the "Program Administrator") is responsible for overall Program management and administration. The Program Administrator shall provide appropriate identity theft training for relevant Berea College employees and provide reports and periodic updates to the Administrative Committee of the College as well as the Audit Committee of the Board of Trustees on at least an annual basis.

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, significant incidents involving identity theft and the College's response, and any recommendations for material changes to this Policy or the Program. As part of the review, Red Flags may be revised, replaced, or eliminated. Defining new Red Flags may also be appropriate.

4.0 Definitions

A **"Creditor"** is any entity that regularly extends, renews or continues credit or regularly arranges for the extension, renewal or continuation of credit.

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.

A **"Customer"** is a person with a Covered Account at the College.

"Identity theft" means fraud committed or attempted using the identifying information of another person without authority.

"Red flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

5.0 Policy

This Policy and the Program apply to all staff, faculty and students and all personnel affiliated with third parties providing services to the College relating to Covered Accounts and/or Sensitive Information within the custody or control of Berea College.

6.0 Sensitive Information to be Protected

A: Personal information upon enrollment, hire or contract:

- Social Security Number
- Date of Birth
- Address
- Phone Numbers
- Maiden Name

B: Payroll Information:

- Same as Personal information along with:
  - Paychecks
  - Pay stubs
  - Any document or electronic file containing salary information

C: Medical Information for employee or student:

- Same as Personal information along with:
  - Doctor names and claims
  - Insurance claims
  - Any personal medical information

D: Credit Card Information, including:

- Credit card number (in part or whole)
- Credit card expiration date
- Cardholder name
- Cardholder address

7.0 Risk Assessment

1. Berea College will consider the following risk factors in identifying Red Flags for Covered Accounts, if appropriate:

a. The types of Covered Accounts we offer or maintain;
b. The methods we provide to open Covered Accounts;
c. The methods we provide to access Covered Accounts; and
d. Our previous experience with identity theft.

2. Berea College will, from time to time, incorporate relevant Red Flags from sources such as:

    a. Incidents of identity theft that we have experienced or that have been experienced by other colleges and universities.
    b. Methods of identity theft identified by us or other Creditors that reflect changes in identity theft risks.
    c. Applicable supervisory guidance.

3. Berea College will, from time to time, include relevant Red Flags from the following categories, if appropriate:

    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.
    e. Notices from customers, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts.

8.0 Protective Actions to be Taken

1. *File cabinets, desk drawers, overhead cabinets and any other storage space containing documents with Sensitive Information will be locked when not in use, at the end of each workday or when unsupervised.*
2. *Writing tablets, post-its, etc. in common shared work areas will be erased, removed or shredded when not in use.*
3. *Sensitive Information to be discarded will be placed in a locked shred bin or immediately shredded using a mechanical cross cut.*
4. *A photo ID will be required any time Sensitive Information related to a Covered Account is collected or changed. Examples include:*

    a. *Charges to Student/Faculty/Staff accounts*
    b. *Student Service Center transactions including loans, check cashing, etc.*
    c. *Seabury Center for membership accounts*

9.0 Detection of Red Flags

Berea College shall address the detection of Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts by:

1. *Obtaining identifying information about and verifying the identity of newly hired employees, newly enrolled students, etc.*
2. *Monitoring transactions through photo ID verification.*
3. *Requiring alternative identification method if photo ID appears to be altered or forged.*
4. *Rejecting any application for a service or transaction that appears to have been altered or forged.*
5. *Including assessment of Red Flags as part of the College's Internal Audit Program.*

10.0 Response to Red Flags

Berea College shall respond quickly to prevent identity theft. ***In all cases report Red Flags to Controller.*** *Response may include:*

1. *Contacting owner of account in question*
    a. *A written letter*
    b. *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. *Determining no response is warranted under the particular circumstances*

11.0 Examples of Red Flags

The following instances are examples of Red Flags recognized by the College:

A: Notifications or warnings from a consumer reporting agency

A.1. A fraud or active duty alert is included with a consumer report;

A.2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;

A.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.

A.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 relationships;
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>

B.1. Documents provided for identification appear to have been altered or forged.
B.2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
B.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.
B.4. Other information on the identification is not consistent with readily accessible information that is on file with us.
B.5. An application appears to have been altered or forged, or given the appearance of having been destroyed and reassembled.

C: <u>Suspicious Personal Identifying Information</u>

C.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.
C.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.
C.3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College, such as:
    a. The address on an application is the same as the 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.

C.4. 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, such as:
    a. The address on an application is fictitious, a mail drop, or a prison; or
    b. The telephone number is invalid, or is associated with a pager or answering device.
C.5. The Social Security Number provided is the same as that submitted by other persons opening an account or is the same as other customers.
C.6. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or is the same or similar to other customers.
C.7. The person opening the Covered Account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
C.8. Personal identifying information provided is not consistent with personal identifying information that is on file at the College.

C.9. If the College uses challenge questions, 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.

D: Unusual use of, or Suspicious Activity Related to, the Covered Account

D.1. Shortly following notice of a change of address for the Covered Account, the College receives a request for a new, additional, or replacement card.

D.2. A new Covered Account is used in a manner commonly associated with known patterns of fraud, such as the customer failing to make the first payment or making an initial payment but no subsequent payments.

D.3. A Covered Account is used in a manner that is not consistent with established patterns of activity on the account, such as:

a. Nonpayment when there is no history of late or missed payments
b. A material increase in the use of available credit
c. A material change in purchasing or spending patterns

D.4. A Covered Account that has been inactive for a reasonably lengthy period of time is used. Determining what is reasonably lengthy should take into consideration the type of account, the expected pattern of usage, and other factors which may be relevant.

D.5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account.

D.6. The College is notified that the customer is not receiving paper account statements.

D.7. The College is notified of unauthorized charges or transactions in connection with a customer's Covered Account.

E: Notice from Customers and Others Regarding Possible Identity Theft In Connection with Covered Accounts Held by the College

E.1. 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.

12.0 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. A service provider that maintains its own identity theft prevention program that is consistent with the policy of the College and the federal law and regulations may be considered to be meeting these requirements. An example of a major service provider could be an external entity that provides student loan administration, billing, reporting, etc.

13.0 Updating the Policy

The Administrative Committee of the College shall annually review this policy and recommend revisions to the Audit Committee of the Board of Trustees when necessary to address changes in risks to students, faculty, staff and all other workers, based on 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

14.0 Program Administration

Training shall be conducted by the Program Administrator for affected students, faculty and staff annually.

For additional information on the FTC's Red Flags Rule please visit the following website:
http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml