# COMPLIANCE PROGRAM

Policy and Procedure — Effective Date: November 30, 2009
Red Flags Identity Theft Policy

**PROGRAM ADOPTION**
Morehouse College ["the College"] has adopted this Identity Theft Prevention Program ["the Program"] pursuant to the Federal Trade Commission's ["FTC"] Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The purpose of the Red Flags Rule is to detect and stop identity thieves from using someone else's identifying information at the College to commit fraud.

This Program was developed with oversight and approval of the Audit Committee of the Board of Trustees. After consideration of the size of the College's operations, account systems, and the nature and scope of the College's activities, the Board of Trustees determined that this Program was appropriate for the College, and therefore approved this Program on _____, 2009.

**POLICY STATEMENT**
It is the policy of the College to protect personal information that it receives, handles, and stores, and to comply with the FTC's Red Flags Rule. The College will collect personal information about individuals only if permissible by law and college policy and when it meets appropriate business purposes. In the event of a security breach involving personal information, any required notifications will be carried out in accordance with College policies and procedures. Therefore, any breach of security or compromise of systems containing personal information must be reported immediately to the CFO or the CFO's designee.

This policy becomes effective November 30, 2009.

**SCOPE AND PURPOSE**
This policy applies to all college departments, administrative units, and affiliated organizations. For the purposes of this policy, affiliated organizations refer to any organization associated with the College that uses the College computer network resources to create, maintain, or store data to perform their business functions.

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered

Formatted: Right: 0.25"

account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts or maintain and incorporate red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identify theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to customers (students/parents/creditors, etc.) and to provide customers with safety and soundness from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

**DEFINITIONS**

**Creditor:** Any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

**Covered Account**: All student loans and/or other accounts that are administered by the College under which multiple payments are made on behalf of the student.

**Red Flag:** A pattern, practice, or specific activity that indicates the possible existence of identity theft.

**Identity Theft:** A fraud which is committed or attempted using identifying information of another person without permission or consent.

**Identifying Information:** Any name or number that may be used alone, or in conjunction with other information, to identify a specific person, including 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 Internet Protocol address, computer access code or secured password.

**Breach of Security:** The unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information of the students, parents or guardians of students, or employees at the College.

**Compromise of Systems:** An apparent exploit of a vulnerability in system software, hardware or a procedural weakness that may provide unauthorized access to the system environment.

Formatted: Right: 0.25"

**Personal Information:** Includes, but is not limited to:

- individual names
- social security numbers
- credit or debit card numbers
- personal/student identification numbers
- driver's license numbers
- dates of birth
- health records when the disclosure of the information in question would reasonably be considered to be harmful or an invasion of privacy.

**REQUIREMENTS OF THE RED FLAGS RULE**

Under the Red Flags Rule, the College is required to develop and implement an "Identity Theft Prevention Program" tailored to its size, complexity and nature of its operation. The Program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program.
2. Detect Red Flags that have been incorporated into the Program.
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
4. Ensure the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the customer from identity theft.
5. Establish guidelines for collecting, retaining, and restricting access to personal information of students.
6. Obtain approval of the Program by the Board of Trustees.

**COVERED ACCOUNTS**

The College has identified 14 types of accounts: eight (8) are covered accounts administered by the College; and six (6) are administered by a service provider.

College covered accounts:

a. Refund of credit balances involving PLUS loans
b. Refund of credit balances excluding PLUS loans
c. Origination of Higher One debit cards for students – IT Department
d. Donations collected by the Office of Institutional Advancement
e. Entry and admission fees collected by the Office of Admissions
f. Credit card use by various campus entities for conferences, programs, and special events.

Service provider covered accounts:

a. Tuition payment plan administered by Sallie Mae Tuition Pay Plan – Independent Contractor
b. Higher Education Services Installment Payment Plan administered by Higher Education Services – Independent Contractor

Formatted: Right: 0.25"

c. Credit card use at parking garage administered by Urban Parking Company – Morehouse Network
d. Credit card use in Café Mazique, Jazzman's Café, and Chivers Dining Hall administered by Sodexho – Independent Contractor
e. Credit card use in campus bookstore administered by Follett – Independent Contractor
f. Credit card use in campus print shop and campus post office administered by Pitney Bowes –Morehouse Network
g. Higher One debit card issued to students administered by Higher One – Independent Contractor
h. Credit/debit card payments to Campus Partners – Independent Contractor

**IDENTIFICATION OF RELEVANT RED FLAGS**

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts, as noted above

2. The methods provided to open covered accounts – acceptance to the College and enrollment in classes requires all of the following information:
   a. Admission application
   b. Common application with personally identifying information
   c. High school transcript
   d. Official ACT or SAT scores
   e. Two letters of recommendation
   f. Entrance Medical Record
   g. Medical history
   h. Immunization history
   i. Insurance card
   j. Photo identification

3. The methods provided to access covered accounts:
   a. Disbursements obtained in person require picture identification
   b. Disbursements obtained by mail can only be mailed to an address on file
   c. Change of address must be in writing with the appropriate signature(s)

4. The College's previous history of identity theft

5. The Program identifies the following red flags:
   1. Documents provided for identification appear to have been altered or forged;
   2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
   3. A request made from a non-College issued e-mail account;
   4. A request to mail something to an address not listed on file;

Formatted: Bullets and Numbering
Formatted: Indent: Left: 1"
Formatted: Right: 0.25"

5. Notice from customers, victims of identity theft, law enforcement authorities,or other persons regarding possible identity theft in connection with covered accounts.

**DETECTION OF RED FLAGS**

Red Flags are indicators of potential fraud. In order to identify relevant Red Flags, the College has reviewed the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. Any time a Red Flag, or a situation closely resembling a Red Flag is apparent, it should be investigated for verification. The College identifies the following Red Flags in each of the listed categories**:**

1. **Refund of a credit balance involving a PLUS Loan –** As directed by federal regulation (USDE), these balances are required to be refunded to the student unless the customer (parent and/or student) completes the appropriate section of the Title IV Form authorizing the College to do one of two things: retain the money in the student's account until further notice or refund the money to the parent. Parent refunds are manual refunds which are handled by the College. These refunds are mailed to the parent after the parent sends written correspondence to Student Accounts giving the name and address of the parent payee. The address should match the address of record on file at the College, and the written correspondence should accompany the submission of the completed Title IV Form to Student Accounts. In unusual circumstances, the parent may be allowed to pick up the check in person, as long as a picture ID issued by a state agency is provided for identity of the parent payee. Personal pick up is not encouraged. **Red Flag – The parental address is different from the address of record at the College. The parent is unable to show a state-issued picture ID.**

2. **Refund of credit balance, no PLUS Loan** – Within 14 days after a credit balance appears on a student's account, refunds are issued to students **automatically** via Higher One. **The College partnered with Higher One to provide disbursement services for all <u>non-parent</u> student refunds**. The vehicle through which these refunds are managed is the Easy Refund Card, a debit card. The initial Easy Refund Card is mailed at no cost to the student's home address of record prior to his arrival at the College (or other address designated by the student over his signature after his arrival at the College) as a first-time student. Literature inside the card mailing instructs the student that prior to receipt of any eligible refund, the student must activate the Easy Refund Card and choose a refund preference. Students have three preferences as to how they wish to receive financial refunds. The three refund preferences are: (1) The Easy Refund One Account -- Place the money on the Easy Refund Card; (2) ACH Transfer - Send the money to a bank; or (3)

Formatted: Right: 0.25"

request a paper check. These refund options are numbered in accordance with the speed in which the refund is available to the student. Preference 1 provides instant access. The student may change his refund preference at any time by logging into his account at www.EasyRefund Card.com and following the prompts. Accounts are protected by a student-selected password.
Refunds to students from the proceeds of the Parent PLUS Loan are managed in the same manner as the refund of credit balances in which no PLUS Loan is involved.

3. Requests from students not currently enrolled or graduated from the college must be made in writing**. Refunds are mailed to students at the address of record at the College or the student must report his current address of record in writing to the Student Accounts Office.** In rare circumstances, non-enrolled students may be allowed to pick up a check if the person is known to Student Accounts and presents a state-issued or College-issued picture ID. **Red Flags – Picture ID not appearing to be authentic or not matching the appearance of the person presenting it**.

4. **Tuition payment plan –** Students must contact an outside service provider and provide personally identifying information to them**. Red Flags – NONE. (See oversight of Service Provider Agreements)**

**RESPONSE**
The Program shall provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft. The appropriate responses to the relevant Red Flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

**OVERSIGHT OF THE PROGRAM**
The responsibility for developing, implementing and updating this program lies with the Vice President for Business and Finance/CFO. The Vice President/CFO is responsible for the Program administration, including ensuring appropriate training of the College's staff, reviewing any staff reports regarding the detection of Red Flags, and taking steps for preventing identity theft.

**REQUIREMENTS FOR COLLECTING, RETAINING AND RESTRICTING ACCESS TO PERSONAL INFORMATION**

Formatted: Right: 0.25"

The College or individual may compile or maintain personal information if required by law or for valid business purposes. In so doing, the College or individual is accountable and will be held responsible for adhering to the following guidelines.

- Maintaining all information on students and employees in a secure fashion in accordance with industry best practices.
- Destroying or arranging for the destruction of personal information of students and employees when there is no longer a legal or business purpose for retention of the information and in conformity with all applicable records retention policies.
- Restricting access to personal information on or about students and employees to only those persons needed to maintain systems, maintain data, meet legal requirements or perform valid business functions.
- Ensuring that file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
- Ensuring that storage rooms containing documents with sensitive information and record retention areas are locked at the end of each workday or when unsupervised.
- Clearing desks and workstations, work areas, common shared work areas, printers and fax machines of all documents containing sensitive information when not in use.
- Erasing, removing, or shredding whiteboards and writing tablets or dry-erasing boards, etc. in common shared work areas when not in use.
- Using a cross cut approved shredding device before discarding documents which contain sensitive information.
- Ensuring that all sensitive information transmitted or electronically stored is encrypted.
- Encrypting and protecting, by password, all sensitive information sent externally and sending to approved recipients only. When sensitive information is sent via e-mail, include this statement: "This message may contain confidential and/or proprietary information and is intended for the person/entity to whom/which it was originally addressed. Any use by others is strictly prohibited."

The College or individual SHALL NOT:

- Publicly post or publicly display, or intentionally communicate or otherwise make available to the general public any personal information of and about students or employees.
- Require an individual to send personal information over the College network unless it meets a valid business purpose and a secure network transmission is used.
- Transfer data containing personal information to anther business unit, private entity or public entity, over the network unless it meets a valid business purpose and a secure network transmission is used.

Formatted: Right: 0.25"

- Mail personal information on a post card or any other mailer not requiring an envelope. Mailed personal information must not be printed on the envelope or visible within unopened envelopes.
- Require an individual to use his or her Social Security number to access an Internet website or other network resource, unless a password or unique personal identification or other authentication device is also required to access the site or resource.
- Display a Social Security number as entered to access an Internet web site or other network resource.
- Print an individual's Social Security number on any materials that are mailed to the individual unless by law, or as part of an application or enrollment process or to establish, amend, or terminate an account, contract or policy, or to confirm accuracy of the Social Security number.
- Print an individual's Social Security number on any card required by the individual to access products or services provided by the College.

**PERIODIC UPDATES TO THE 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 accounts covered by the Program. As part of the review, Red Flags may be revised, replaced or eliminated. Redefining 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, its students and employees.

**STAFF TRAINING**

Staff training will be conducted for all requisite employees. Employees must receive annual training in all elements of this policy in the detection of Red Flags, including the responsive steps to be taken when a Red Flag is detected. To ensure maximum effectiveness, employees will continue to receive additional training as changes to the Program are made.

**OVERSIGHT OF SERVICE PROVIDER AGREEMENTS**

The College shall take steps to ensure that the activities of service providers are conducted in accordance with reasonable policies and procedures. The policies and procedures will be designed to detect, prevent and mitigate the risk of identity theft whenever the College engages a service provider to perform an activity in connection with one or more covered accounts. The College will maintain on file **certification**s from all third party administrators that they are PCI compliant.

Currently the College has service provider agreements with the following agencies:

- Student Refund Management
  HigherOne, Inc. [www.EasyRefundCard.com, 877-327-9515]
- Tuition Payment Plans
  Sallie Mae Tuition Pay Plan [www.tuitionpay.com, 800-635-0120]

Formatted: Right: 0.25"

Higher Education Services Installment Payment Plan
[www.highereducationservices.org, 800-422-0010]

- Billing Agency for Perkins Loan
  Campus Partners [www.mycampusloan.com, 800-334-8609]

To receive or participate in the service, the students contact these agencies directly online or by telephone/letter, providing personally identifying. The identifying information is matched to the records that the College has provided to these organizations.

Formatted: Right: 0.25"