APPROVAL OF AN IDENTITY THEFT PREVENTION PROGRAM

RESOLUTION NUMBER 2009–54

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, required the promulgation of federal rules regarding identity theft protection, and

WHEREAS, the federal rules, as promulgated by the Federal Trade Commission, the federal bank regulatory agencies, and the National Credit Union Administration, require Ivy Tech Community College Indiana to implement an identity theft prevention program, and

WHEREAS, the date by which the College must comply with the federal rules is November 1, 2009, and

WHEREAS, responsibility for developing, implementing, and updating this program lies with an Identity Theft Committee consisting of College employees representing the Office of the President, the Office of the Provost, and the Office of the General Counsel, and they have developed the Identity Theft Prevention Program and the Red Flag Policy set forth in Exhibit A, which is attached to and made a part of this resolution, and

WHEREAS, the State Board of Trustees has determined that approval of the Identity Theft Prevention Program and the Red Flag Policy is in the best interest of the College and its students;

NOW THEREFORE BE IT RESOLVED, that the State Trustees approve the Identity Theft Prevention Program and the Red Flag Policy set forth in Exhibit A.

State Trustees
Ivy Tech Community College of Indiana

Kaye H. Whitehead, Chairman

Anne K. Shane, Secretary

Dated October 15, 2009
EU1.10 Identity Theft Prevention Program/Red Flag Policy

**Principle:**
Ivy Tech Community College of Indiana ("College") developed this Identity Theft Prevention Program ("Program") in compliance with part 681 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 and pursuant to the Federal Trade Commission’s (FTC) Red Flags Rule ("Rule"), the Ivy Tech Community College Board of Trustees has adopted the following Identity Theft and Red Flag Policy. This Program was developed with oversight and approval of the Ivy Tech Community College State Board of Trustees, Office of the President, Office of the Provost, and Office of General Counsel. After consideration of the size and complexity of the College’s operations and account systems, and the nature and scope of the College’s activities, the Ivy Tech Community College State Boards of Trustees determined that this Program was appropriate for the College, and therefore approved this Program on October 14, 2009.

**Objective:**
The Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program established procedures to:
1. Identify relevant red flags for covered accounts it offers or maintains 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 flag that has been detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the creditor from identity theft.

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

**Approval Authority:** The State Board of Trustees for the initial issuance of this policy. The Identity Theft Committee for any subsequent revision to this policy.

**Responsible Executive:** Vice President/Treasurer

**Responsible Office:** College Finance Office

**Originally Issued:** November 1, 2009

**Policy:**
It is Ivy Tech Community College’s policy to assist in the prevention and detection of identity theft. The college is adopting this Red Flag Detection and Reporting Policy to assist in the detection, protection and mitigation of identity theft pursuant to the red flag regulations issued by the Federal Trade Commission. This policy covers all students, employees and contractors of Ivy Tech Community College.
I. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

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

A “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

A “Covered Account” includes all accounts or loans that are administered by the College.

A “Program Administrator” is the individual designated with primary responsibility for oversight of the program.

“Identifying information” is “any name or number that may be used 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.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each 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; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees, or to the safety and soundness of the student or employees accounts from Identity Theft.

II. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the College considers 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. The College identifies the following Red Flags in each of the listed categories:
A. Notifications and Warning from Credit Reporting Agencies

**Red Flags**

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity.

B. Suspicious Documents

**Red Flags**

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document.
3. Other document with information that is not consistent with existing student or employee information; and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

**Red Flags**

1. Identifying information presented that is inconsistent with other information the employee or student provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another employee or student;

6. A person fails to provide complete personal identifying information on an application when reminded to do so; and

7. A person’s identifying information is not consistent with the information that is on file for the employee or student.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Changes of address for an account followed by a request to change the student’s or employee’s name;

2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use;

4. Mail sent to the student is repeatedly returned as undeliverable;

5. Notice to the College that a student is not receiving mail sent by the College;

6. Notice to the College that an account has unauthorized activity;

7. Breach in the College’s computer system security; and

8. Unauthorized access to or use of student account information.

E. Alerts from Others

Red Flags

1. Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

III. DETECTING RED FLAGS

A. ID Card Issuance

In order to detect any of the Red Flags identified above associated with the issuance of an ID card, College personnel will take the following steps to obtain and verify the identity of the person requesting the card:
Detect

1. Require certain identifying information such as name, date of birth, home address or other information; and

2. Verify the student or employee’s identity at time of issuance of the identification card (review of driver’s license or other government-issued photo identification).

B. Student and Employee Covered Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students or employee if they request information (in person, via telephone, via facsimile, via email);

2. Verify the validity of requests to change billing addresses by mail or email and provide the student or employee a reasonable means of promptly reporting incorrect billing address changes; and

3. Verify the identity of students or employees changing banking information given for billing and payment purposes.

C. Consumer (“Credit”) Report Requests

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

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

2. 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 the College has reasonably confirmed is accurate.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event College 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:
Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft and document all actions taken;

2. Change any passwords or other security devices that permit access to Covered Accounts;

3. Not open a new Covered Account;

4. Provide the student with a new student identification number;

5. Notify the Program Administrator for determination of the appropriate step(s) to take;

6. Notify law enforcement;

7. File or assist in filing an Ivy Tech Incident Response Checklist; or

8. Determine that no response is warranted under the particular circumstances.

Protect Student and Employee Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;

2. Ensure complete and secure destruction of paper documents and computer files containing student or employee account information when a decision has been made to no longer maintain such information;

3. Ensure that office computers with access to Covered Account information are password protected;

4. Avoid use of social security numbers, unless required by law;

5. Ensure computer virus protection is up to date; and

6. Require and keep only the kind of student or employee information that is necessary for College purposes.
V. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) for the College. The Committee is headed by a Program Administrator who will be appointed by the President of the College. The Committee will consist of one representative from each of the following areas: Legal, Finance, Human Resources, Student, Information Security, and Internal Audit.

B. Staff Training and Reports

College 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. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the College’s failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, College 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, significant incidents involving identity theft and management’s response, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College 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.

1. Require, by contract, that service providers have such policies and procedures in place; and

2. Require, by contract, that service providers review the College’s Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship.

D. 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 the Committee who developed this Program and 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 “sensitive” as defined by the College data classification policy.

E. Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students or employees and the soundness of the College from Identity Theft. In doing so, the Committee will consider the College’s experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College’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.

Commentary:
This policy should be read in conjunction with the college’s Information Classification Policy (SM1.1). If an employee is uncertain of the sensitivity of a particular piece of information, they should contact their immediate supervisor for clarification.

Confidential Information for the Purpose of the College’s Identify Theft and Red Flag Policy
Confidential Information includes data covered by Federal and State legislation such as FERPA and the Data Protection Act or is legally covered by contract and must be protected at all times. The disclosure of this information may seriously damage or negatively impact the College.

Definition of Confidential Information
Confidential Information includes, but is not limited to, the following items whether stored in electronic or printed format:

Credit and debit card information, including:
1. Credit and debit card number (in part or whole)
2. Credit and debit card expiration date
3. Cardholder name
4. Cardholder address

Tax identification numbers, including:
1. Social Security number
2. Business identification number
3. Employer identification number

Personnel & Payroll information, including among other information:
1. Paychecks
2. Pay stubs
3. W-2’s
4. Vendor remittances for employee benefits
Personal banking information for any employee, student, customer, or constituent, including but not limited to:

1. Password/Log-In information for online banking.
2. Bank account number.
3. Routing number.

Other Information Commonly Used in Identity Theft
The following information, even though it may otherwise be considered public or proprietary, is often used in conjunction with Confidential Information to commit fraudulent activity such as identity theft:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number
7. Driver's License Number

Hard Copy Distribution and Storage
All College personnel shall comply with the following requirements:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Confidential or Sensitive Information must be locked when not in use.
2. Storage rooms containing documents with Confidential or Sensitive Information and record retention areas must be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleaned of all documents containing Confidential or Sensitive Information when not in use.
4. Whiteboards, dry erase boards, writing tablets, etc. in common shared work areas containing Confidential or Sensitive Information must be erased, removed, or shredded when not in use.
5. College records may only be destroyed in accordance with the College’s records retention policy and applicable law (SM1.16).
6. Documents containing Confidential Information must be disposed of in a secure manner. A secure manner includes destroying the documents using a cross-cut shredder or disposing of documents in an authorized disposal container.

Electronic Distribution and Storage
All College employees shall comply with the following policies:

1. Non-College email systems, including but not limited to, Hotmail, Yahoo, and/or Google shall not be used to send Confidential or Sensitive Information. When using approved College e-mail systems to send Confidential or Sensitive Information internally the preferred mode is to encrypt or password protect such information (EU1.5).
2. Any Confidential Information sent to recipients externally (i.e. to non Ivy Tech Community College email accounts) should be encrypted and sent only to approved recipients.
Additionally, a statement such as this should be included in the e-mail:
"The information contained in this transmission may contain privileged and confidential information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message."

3. Encryption technologies should be employed when Confidential Information is being stored on mobile devices such as laptops, backup media, DVDs, CDs, external hard drives, and thumb drives, among others (EU1.5).

4. Confidential Information should be encrypted when internally transmitted over an electronic communications network.

5. All hardware/storage media that will be repurposed for use within the College must be sanitized adhering to Ivy Tech Community College’s Data Disposal Policy (SM1.16). The Policy recommends the approach of overwriting all addressable media locations, a minimum of three times, with a character, its complement, then a random character and verifying the process. If hardware will be disposed of, or will be transferred to a third party outside of the College, all storage media must be rendered unusable, adhering to government standards which requires degaussing and/or complete physical destruction.

Application of Other Laws and College Policies
College personnel should make reasonable efforts to secure Confidential or Sensitive Information to the proper extent. Furthermore, this section should be read and applied in conjunction with applicable laws and College policies. If an employee is uncertain of the Red Flag implications of a certain piece of information, he/she should contact the appropriate regional senior level manager or the specific department within the Office of the President or Office of the Provost.

Procedure:

A. Covered Accounts
   College administered covered accounts - Students
      1. Plus Loans
      2. Stafford Loans
      3. College Institutional Loans
      4. Deferred Tuition Payments
      5. HigherOne card balances
      6. Student Account Receivables
      7. Contract Account Receivables

   College administered covered accounts - Employee
      i. Employee Payroll
      ii. Employee Reimbursements
      iii. Direct Deposit information
Risk Assessment
For the student related College administered covered accounts listed above, the existing risk is that a fraudulent request is made for a refund on an overpaid account resulting from a loan and/or direct payment. Since the College is solely responsible for issuing refunds on these accounts, the risk resides at the College level.

There is no perceived risk associated with the employee payroll and reimbursement programs. When funds are owed to the employee, the funds would be returned to the employee through the standard payment process. This process maintains its own control structure to ensure proper payment to employees.

The College will take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. However, the processes transacted by these providers represent funds owed to the College, mitigating the risk of theft to the account holders. Additionally, the College will take steps to review the Red Flag policies and procedures enacted by these providers.

Control Procedures
As noted above, the primary risk associated with the covered accounts relates to refunds on student accounts and loan accounts. The following control procedures mitigate this risk:

The College will initiate a refund on all student accounts that are in an overpaid status to the most current address on file.

Checks and HigherOne debit cards are mailed to the official name and address within the College’s Information System or may be picked up in person. The student must provide a valid picture ID when receiving the check in person.

Non-employee students must make all name change requests to the Registrar’s Office. Students who are also College employees must make all name change requests to the Human Resources Office. A change in name requires the appropriate legal document. These changes require the student to visit the Registrar’s Office in person and present a valid picture ID. A change in address may be requested either through the student’s Campus Connect account or in person. If requested in person, the student must show a valid picture ID.

Red Flags
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.

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

**Response to Red Flags**
The program provides appropriate responses to detect 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 or employee;
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.