WESTMONT COLLEGE IDENTITY THEFT PROGRAM

Westmont College ("the College") is committed to taking all reasonable and appropriate measures to prevent identity theft. To that end, and in keeping with the Federal Trade Commission's (FTC) Red Flag Rules,[1] the college developed this program to detect, prevent and mitigate instances of identity theft[2] in connection with personally identifiable information[3] the college maintains; and information received or activity observed related to the same information that signals potential identity theft. The College Board of Trustees determined that this Program was appropriate, and therefore approved this Program on May 8, 2009. This program is administered by the Vice President for Administration.

I. IDENTIFYING POTENTIAL IDENTITY THEFT

Upon offering, opening and maintaining covered accounts[4] the college will review personally identifiable information presented for suspicious activity that signals potential identity theft. These ***red flag alerts*** include but are not limited to:

- Loan or tuition account documents presented with inaccurate, inconsistent or non-matching personally identifiable information
- Repeated return of undeliverable mail addressed to the account holder
- Sudden and repeated delinquent payments on an otherwise consistently current covered account
- Receipt of notice from the account holder that identity theft has occurred
- Receipt of a credit report obtained in connection with an employment offer that contains a fraud alert
- Photo identification presented that is inconsistent with the person presenting the document
- Receipt of documents that appear to be forged or altered

---

[1] The FTC's Red Flag Rules implement section 114 of the Fair and Accurate Credit Transactions Act of 2003. A Red Flag alert is defined as a pattern or practice or specific activity that indicates the possible existence of identity theft.

[2] Identity theft is a fraud committed or attempted using the identifying information of another of another person.

[3] Personally identifiable information is any name or number that may be used, alone or in conjunction with any other information to identify a specific person. For purposes of this program, "personally identifiable information" includes but is not limited to the following:

- Social Security Number
- Student Identification Number
- Driver's License Number
- Government Issued Identification Card Number
- Financial Account Number (e.g. tuition account number)
- Credit/Debit Card Number
- Personal Identification Number associated with a financial/credit/debit account number
- Bank Routing information
- Computer Log in and Password Information

[4] A covered account includes all accounts or loans where payment is deferred for services.

II. DETECTING RED FLAG ALERTS

The college will take one or more of the following steps in order to detect the red flags described above

- Verification of identify with required government issued identification (e.g., driver's license, social security card, state issued identification card)
- Verification of identity prior to issuing employee or student identification card
- Verification of identity prior to providing covered account information
- Verification of personally identifiable information presented

III. PREVENTING AND MITIGATING IDENTITY THEFT

Upon detection of circumstances constituting a red flag alert or where personally-identifiable and unencrypted information, in electronic or paper form has been or may have been accessed by someone without authority, the college will take one or more of the following actions:

- Routinely monitor covered accounts for red flags
- Password protect all covered accounts
- Preserve the security of the college website and/or provide notice when security has been compromised
- Notify the holder of the individual account to inform him/her of the activity or incident signaling potential fraud
- Not open covered accounts until all identification discrepancies are resolved
- Provide student or employee with new identification number where original number has been compromised
- Change account holders internet protocol in connection with covered account
- Routinely and securely destroy paper documents bearing personally identifiable information
- Provide victim of identity theft with information on state and federal agencies designed to mitigate identity theft and recover identity (e.g., California Office of Privacy Protection, Federal Trade Commission)
- Notify law enforcement where appropriate
- Determine other appropriate response to the red flag alert not listed

All known or potential incidents of identity theft are to be reported to the Vice President for Administration, who will alert the Vice President for Information Technology and CIO, and College Counsel.

IV. PROGRAM ADMINISTRATION

A. Program Oversight and Updates

Responsibility for developing, implementing and updating this Program lies with the Vice President for Administration (the "Program Administrator") in consultation with the Vice President for Information Technology and CIO, and College Counsel. The program administrator will be responsible for ensuring college employees are appropriately trained on the program, reviewing reports of any red flags, and determining which steps of prevention and mitigation are appropriate under the circumstances. The program administrator is also responsible for routinely reviewing the program to determine what if any changes are necessary or appropriate.

B. Staff Training and Reports

College staff with responsibility for opening, maintaining and monitoring covered accounts; or for managing personally identifiable information shall be trained by the program administrator in the detection of red flag. Staff will notify the program administrator upon receipt of information signaling identity theft. Annually, directors of areas of staff with responsibility for covered accounts and identifiable information shall report to the program administrator on the effectiveness of the identity theft program.

C. Service Provider Oversight

In the event the college engages a service provider to perform an activity in connection with covered accounts, the college will take the following steps to ensure the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

- Require service providers to have policies to identify, prevent and mitigate identity theft
- Require that service providers have determined the red flags that might occur in the course of their providing services under their contracts
- Require that service providers review the college's list of red flag alerts and report any instances to the program administrator