Gettysburg College

Identity Theft Prevention (Red Flags) Policy

Adopted by the Board of Trustees October 2, 2010
Updated by the Board of Trustees May 2016

Policy Statement

Gettysburg College (the College) endeavors to safeguard personal and private information of all of its constituents, including faculty, staff, students, vendors, volunteers, and donors in accordance with its Information Management Policy. Additionally, in its role as creditor, the College understands the importance of complying with applicable federal regulations under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) to establish an Identity Theft Prevention Program designed to identify and detect relevant warning signs, or red flags, of identity theft.

The purpose of this policy is to establish an Identity Theft Prevention (Red Flags) Program (the Program) which will include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program.
2. Detect and record 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. Respond appropriately to address discrepancy notices from national consumer credit reporting agencies received by the College.
5. Ensure the Program is updated periodically to reflect changes in identity theft risks and applicable best practices.

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

Definitions

- *Identity Theft* - Fraud committed or attempted using identifying information of another person without authority.
- *Red Flag* - Pattern, practice, or specific activity that indicates the possible existence of identity theft.
- *Covered Accounts* - Any consumer account that the College offers in its capacity as creditor that is designed to permit installment payments or any other financial account offered or maintained by the College for which there is reasonably foreseeable risk of identity theft.

Identification of Relevant Red Flags

1. The Program shall include relevant Red Flags from the following categories as appropriate:
    a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.
    b. The presentation of suspicious documents.
    c. The presentation of suspicious personal identifying information.
    d. The unusual use of, or other suspicious activity related to, a covered account.
    e. Notice from College constituencies, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

2. The Program shall consider the following risk factors in identifying relevant Red Flags for covered accounts as appropriate:
    a. The types of covered accounts offered or maintained.
    b. The methods provided to open covered accounts.
    c. The methods provided to access covered accounts.
    d. Its previous experience with identity theft.

3. The Program shall incorporate relevant Red Flags from sources such as:
    a. Incidents of identity theft previously experienced.
    b. Methods of identity theft that reflect changes in risk.
    c. Applicable regulatory or professional guidance.

Detection of Red Flags

The Program shall address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account.
2. Authenticating "customers", monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Response to Red Flags

The Program shall provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft.
2. Contact the "customer" or actual account holder that fraud has been attempted.
3. Change any passwords, identification numbers, or other security devices that permit access to the covered accounts.
4. Reopen a covered account with a new account number.
5. Not open a new covered account.
6. Cancel the transaction and/or close the account.
7. Notify and cooperate with appropriate law enforcement.
8. Determine that no response is warranted under the particular circumstances.

Duties Regarding Address Discrepancies

If the organization receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report, the Program shall be designed to enable the College to form a reasonable belief that a credit report relates to the consumer for whom it was requested.

Service Provider Arrangements

The College shall 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. Each engaging department will be responsible to exercise appropriate and effective oversight of their service provider arrangements in accordance with this Program.

Administration of the Program

1. *Development, Implementation, and Oversight*: With oversight and authorization by President's Council, the Ethics and Integrity Committee shall be responsible for developing, implementing, and operational oversight of the Program. Specifically, the Associate Vice President of Information Technology, Co-Director of Human Resources and Risk Management, and Director of Financial Services/Controller (Designated Authorities) as members of the Ethics and Integrity Committee and by nature of respective positions, will coordinate efforts of the Program. President's Council Oversight of the Program shall include:
    a. Assignment of specific responsibility for implementation of the Program.
    b. Review of reports prepared by staff regarding compliance.
    c. Approval of material changes to the Program as necessary to address changing risks of identity theft.

2. *Training:* Ethics and Integrity Committee members shall train staff, as necessary, to implement the Program effectively within the individual departments' needs.

3. *Program Review and Updates:* The Program shall be reviewed and updated periodically to reflect changes in risks to "customers" or to the safety and soundness of the College from identity theft. In doing so, the Ethics and Integrity Committee will consider the following:

a. The experiences of the College with identity theft.
b. Changes in methods of identity theft.
c. Changes in methods to detect, prevent and mitigate identity theft.
d. Changes in the types of accounts that the organization offers or maintains.
e. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

4. *Reporting:* The Designated Authorities will provide a written report annually to the Ethics and Integrity Committee concerning compliance by the organization with the Program and, and recommendations for continued administration of the Program. President's Council will be notified immediately of incidents involving identity theft and management's response.