GOUCHER | college

Identity Theft Prevention Program

I. PROGRAM ADOPTION

Goucher College (the "College") developed this Identity Theft Prevention Program ("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. This Program was developed with oversight and approval of the Executive Committee of the Board of Trustees of Goucher College. 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 Board of Trustees determined that this Program was appropriate for the College, and therefore approved this Program on March 24, 2009.

II. DEFINITIONS

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

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

"College Covered Account" includes all student accounts or loans that are administered by the College, including but not limited to, federal, state, institutional and private loan accounts, student accounts that may, from time to time, have credit balances to be reimbursed, and OneCard accounts.

"Service Provider Covered Account" includes student accounts or loans that are administered by an outside entity with which the college has contracted, including the tuition payment plan administered by TuitionPay and student loan program administered by ACS.

"Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VII below.

"Identifying information" is any name or number that may be used, alone or in conjunction with any 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, and computer's Internet Protocol address, or routing code.

III. PURPOSE OF THE PROGRAM

The purpose of the Identity Theft Prevention Program is to enable the College to detect, prevent and mitigate identity theft in connection with the opening of a College Covered Account or with an existing College Covered Account or Service Provider Covered Account, and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. identify relevant types of Red Flags for new and existing College Covered Accounts and incorporate those Red Flags into the Program;
2. detect Red Flags of the type 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 from Identity Theft.

IV. IDENTIFICATION OF RED FLAGS

A. Risk Assessment

In order to identify relevant types of Red Flags, the College considers the following information:

1. the types of College Covered Accounts that it offers and maintains (described above);
2. the methods it provides to open College Covered Accounts;
    - Covered accounts are opened only for individuals that enroll as students at the college. It is very unlikely that Identity Theft will be committed in connection with the opening of a Covered Account, given the large amount of information that must be submitted to the College by the time an accepted student enrolls, including:
        i. the common application
        ii. high school transcript
        iii. letters of recommendation
        iv. medical records
        v. insurance card
        vi. financial aid applications, including the FAFSA and CSS profile
    - Creation of a OneCard Account for enrolled students requires presentation of a picture identification card and verification of enrollment. http://www.goucher.edu/x3862.xml and http://www.goucher.edu/x3859.xml.
3. the methods it provides to access its College Covered Accounts;
    - Disbursements from Covered Accounts obtained in person require picture identification and signature.
    - Disbursements obtained by mail can be mailed only to an address on file.

- Transfers are made from one Covered Account to another (e.g., from the student's billing account to the student's OneCard account) only upon written request from the account holder.
- Address changes for a billing account are processed only if requests are received in writing or from a Goucher email account of the account-holder.

4. its previous experiences with Identity Theft (Goucher has received no reports of Identity Theft involving any Covered Account within the memory of current registration, billing, or financial aid staff).

B. Identification of Relevant Red Flags

The Program shall include the following Red Flags:

1. alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. the presentation of suspicious documents, such as documents appearing altered or forged;
3. the presentation of suspicious personal identifying information, such as a photograph or physical description on an identification card that is not consistent with the appearance of the student presenting the identification;
4. a request to mail something to an address not listed on file;
5. the unusual use of, or other suspicious activity related to, a College Covered Account;
6. notice from customers, victims of Identity Theft, law enforcement authorities, NSLDS, or other persons regarding possible Identity Theft in connection with College Covered Accounts;
7. breach in the College's computer system security; and
8. unauthorized access to or use of College Covered Accounts.

V. DETECTING RED FLAGS

The Program shall address the detection of Red Flags in connection with the opening of College Covered Accounts and existing College Covered Accounts.

A. Creation of New Accounts

In order to detect any of the Red Flags identified above associated with the enrollment of a student and creation of a new student College Covered Account, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Through the Admissions process, require certain identifying information such as name, date of birth, academic records, home address, or other identification; and
2. Verify the student's enrollment and identity at time of issuance of a new student OneCard (review of driver's license or other government-issued photo identification) and verification of enrollment at time of issuance of a replacement OneCard. See http://www.goucher.edu/x3859.xml and http://www.goucher.edu/x3862.xml.

B. Existing Accounts

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

1. obtain identifying information about, and verify the identity of, a person accessing a College Covered Account (electronically by use of a PIN, and in personby requiring production of photo identification);
2. verify the validity of change of address requests with the Registrar's office;
3. require that all requests for refunds from Covered Accounts be initiated by the account-holder only and require authorization of a Vice President for all refunds over $5,000; and
4. deactivate OneCards within one week of a student's graduation, withdrawal, or leave of absence from the College.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

A. Responding to Red Flags

In the event College personnel detect any identified Red Flags, such personnel shall notify the Program Administrator of the Red Flag and, in consultation with the Program Administrator, take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. monitor the College Covered Account for evidence of Identity Theft;
2. deny access to the College Covered Account until other information is available to eliminate the Red Flag, or close the existing College Covered Account;
3. contact the student;
4. change any passwords, security codes, or other security devices that permit access to the College Covered Account;
5. reopen the College Covered Account with a new account number;
6. notify law enforcement; or
7. determine no response is warranted under the particular circumstances.

B. Protecting Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to College 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 account information when a decision has been made to no longer maintain such information;
3. ensure that office computers and other electronic devices with access to College Covered Account information are password protected;
4. avoid use of social security numbers whenever possible;
5. ensure computer virus protection is up to date; and

6. encourage account-holders to frequently monitor Covered Accounts for unauthorized activity.

VII. PROGRAM ADMINISTRATION

A. Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the Office of General Counsel, which shall be the Program Administrator. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program.

B. Staff Training and Reports

1. 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.
2. College employees are expected to notify the Program Administrator in writing or via email if they detect an identified Red Flag, or become aware of an incident of Identity Theft or of the College's failure to comply with this Program.
3. Upon request, College staff responsible for development, implementation, and administration of this Program shall report to the Program Administrator on compliance with the Program. The report shall address material matters related to the Program, and evaluate issues such as the effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with College Covered Accounts, significant incidents involving Identity Theft and management's response, and recommendations for changes to the Program.

C. 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 College engages a service provider to perform an activity in connection with one or more College Covered Accounts.

Currently the College uses TuitionPay to administer the Tuition Payment Plan and ACS to administer the Perkins and Goucher Loans. Students contact TuitionPay and ACS directly through their websites or by telephone and provide personally identifying information to be matched to the records that the College has provided to these entities.

D. Updating the Program

The Program will be periodically reviewed and updated to reflect changes in risks from Identity Theft. At least once per year in May, the Program Administrator will consider the College's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the College maintains 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 identification of Red Flags in IV.B, are warranted. If warranted, the Program Administrator will update the Program and submit such updated program to the Board of Trustees for approval.