GOUCHER | college

Red Flag Program Policy and Procedure

I. WHAT ARE THE "RED FLAG RULES"?

Red Flag Rules are the shorthand name for regulations issued by The Federal Trade Commission (FTC) that require financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003.

The regulations were issued to address the serious problem of identity theft, in which identity thieves use people's personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses.

Financial institutions and creditors are required to implement a "red flags" program to detect, prevent, and mitigate instances of identity theft. Programs were put in place by May 1, 2009, and were to provide for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

II. WHO MUST COMPLY WITH THE RED FLAG RULES?

The Red Flag Rules apply to "financial institutions" and "creditors" with "covered accounts." Although colleges are not considered "financial institutions" or "creditors" as those terms are ordinarily used, Goucher (and other colleges and universities) meets those definitions as they are used in the regulations.

Goucher is a "financial institution" because it holds accounts belonging to "consumers" (Goucher students). Goucher is also considered a "creditor" because it provides loans to students and arranges for the provision of loans by other entities.

Goucher has identified "covered accounts" for which it must have Red Flag rules as student accounts and loans that are administered by the College, and OneCard accounts.

III. WHAT RED FLAGS HAS THE COLLEGE IDENTIFIED IN ITS PROGRAM?

Goucher has identified eight red flags that could indicate that identity theft has occurred in connection with one of its covered accounts. They are:

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 a College Covered Accounts.

IV. HOW WILL GOUCHER DETECT THAT RED FLAGS EXIST?

It is possible, though extremely unlikely, that a student account may be created in connection with attempted identity theft. The College’s admission process requires the provision of a significant amount of information that would make it unlikely for an account to be opened and used to commit identify theft. Nevertheless, the College will take steps to obtain and verify the identity of all students who open loan or other accounts or OneCard accounts with the College so as to detect potential Red Flags.

In order to detect any of the Red Flags for existing accounts, college personnel will monitor transactions on accounts, including, for example, verifying the validity of change of address requests with the Registrar’s office so that personal information is not inadvertently sent to someone who is trying to commit identify theft.

V. HOW WILL GOUCHER PREVENT AND MITIGATE IDENTIFY THEFT AT THE COLLEGE?

The College intends to prevent instances of identity theft by ensuring that its website is secure, properly disposing of paper and digital files that contain sensitive information, ensuring that office computers and other electronic devices with access to College Covered Account information are password protected, avoiding use of social security numbers whenever possible, ensuring that computer virus protection is up to date, and encouraging account holders to frequently monitor Covered Accounts for unauthorized activity.

In the event college personnel detect any identified Red Flags, such personnel shall notify the Director of Risk Management & Contracts r of the Red Flag and, in consultation with the the Director of Risk Management & Contracts, take one or more steps to mitigate the identify theft depending on the degree of risk posed by the Red Flag, such as monitoring an account, denying access to an account, or closing an account.

VI. WHO IS IN CHARGE OF THE COLLEGE’S RED FLAGS PROGRAM?

Responsibility for developing, implementing and updating this Program lies with the Office of Finance and Risk Management & Contracts. The offices of Finance and Risk Management are responsible for ensuring appropriate training of college staff, 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.

The Director of Risk Management and Contracts will periodically review the program, update the Program if necessary, and submit such updated program to the Board of Trustees for approval.

VII. RESPONSIBLE OFFICE

For more information or if you have questions about this policy, please contact the Director of Risk Management & Contracts at risk.management@goucher.edu.

VIII. HISTORY

Updated: August 2019; June 2023