SIMMONS UNIVERSITY
OFFICE OF THE GENERAL COUNSEL

"RED FLAG RULE" POLICY

Background of the Federal Legislation Known as "Red Flag Rule"

The Federal Trade Commission (FTC) has issued a regulation known as the Red Flag Rule (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act) to reduce identity theft. The Red Flag Rule is intended to detect, prevent and mitigate opportunities for identity theft. Simmons University is subject to this federal law and must develop and implement a written Identity Theft Protection Program to protect our constituencies and comply with the law.

Why Does This Law Apply to Simmons?

The Red Flag Rule applies to "financial institutions" and "creditors" with "covered accounts." Although at first glance, universities and colleges do not appear to fall within the scope of the legislation, we know that Simmons fits the criteria because:

- We participate in the Federal Perkins Loan Program;
- We participate as a school lender in the Direct Lending Program;
- We offer institutional student loan programs;
- We offer a payment program through a third party;
- We hold payment plans and promissory notes for covered student accounts;
- In employee hiring process and for students in certain programs, we perform background checks and receive credit reports; and
- We use databases throughout the University that contain sensitive information on students, employees, alumni and donors.

What is the Purpose of Instituting This Policy at Simmons?

Many offices throughout Simmons University hold sensitive information, as defined by the Red Flag Rules. We are enacting this policy to protect our students, employees, contractors, alumni and donors from identity theft in accordance with Federal law. We are also adopting this policy to mitigate the potential for damages related to the loss or misuse of sensitive information.

More specifically, this policy will:

- Define "sensitive information" covered by the Red Flag Rule;
- Describe proper protocols for physical data security when stored and distributed;
- Describe proper protocols for electronic data security when stored and distributed;
- Identify risks in new/existing covered accounts that signify potentially fraudulent activity;
- Provide proper protocol for responding to risk if fraudulent activity has occurred; and
- Place us in compliance with the Red Flag Rule and reducing/managing risk.

What is Sensitive Information and How Does This Policy Apply to Me?

Sensitive information is personal information belonging to any student, donor, employee, contractor, alumni, or other constituent of Simmons University. This information may include, but is not limited to, social security numbers, medical information, payroll and benefits information, tax identification numbers, credit card information, etc. As a Simmons employee you may be privy to sensitive information in the course of your job. You are expected to comply with the University's data security policies, processes, and expectations in securing confidential information.

What are Some Examples of Sensitive Information I May Encounter?

Below are examples of common sensitive information typically found in departments of the University. This list is not all inclusive. All offices across the University must be mindful of confidentiality and protecting sensitive information. If you need clarification on what constitutes sensitive information, it is your responsibility to seek it from your direct supervisor.

For example:

If you work in any **Admission Office** across the University:

- Student personal information including address, date of birth, contact information, and academic information protected under state or federal law, such as the Family Education Rights and Practices Act (FERPA)

If you work in **Advancement:**

- Donor information, including address, asset information, financial data, business identification numbers, employer identification numbers, and credit card information

If you work in the **Campus Card Office**:

- Credit Card information, including card number, cardholder name and address

If you work in **Health Services** or the **Counseling Center:**

- Medical information, including doctor names, insurance claims, prescriptions and other personal medical information

If you work in **Human Resources:**

- Personal information for employees, such as social security number, address, other contact information, results of background and credit checks, and benefits statements/information

If you work in **Payroll:**

- Payroll information including social security numbers, paychecks, salary data, paystubs, and benefits statements

If you work in **Student Financial Services:**

- Tax identification numbers, parent and student tax information, business identification numbers, and employer identification numbers

If you work in the **Registrar's Office:**

- Academic Records or other data protected under state or Federal laws, such as FERPA

What are some Specific Potential Red Flags?

The following have been identified as potential indicators of Red Flag activity. Please keep in mind that this list is not all inclusive and it is your responsibility as a Simmons University employee to use common sense judgment and reasonable efforts, and err on the side of caution, in order to identify potential Red Flags.

- The Social Security number provided is the same as that submitted by another person with an account held by Simmons
- Address discrepancies noted in background check reports
- Students, applicants or employees offering suspicious documents
- Photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification
- Personal identifying information provided is not consistent with other personal identifying information on file with the University
- Documents provided for identification appear to have been altered or forged
- Notification from students, borrowers, law enforcement, or service providers of unusual activity related to a covered account
- Notification from a credit bureau of fraudulent activity

- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor
- An application or transcript appears to have been altered or forged, or appears to have been destroyed and reassembled
- The University is notified that a borrower or student has not been receiving paper account statements
- Simmons is notified of unauthorized charges or transactions in connection with a student or borrower account
- A student account is used in a manner commonly associated with known patterns of fraud
- Change of address for an account is immediately followed by a request to change the student's name
- There is a breach in the University's computer system
- There is unauthorized access or use of student accounts
- Payments stop on an account that is otherwise consistently up-to-date

If I Identify a Potential Red Flag, How do I Proceed?

If you believe you have identified a Red Flag, please take the following steps to ensure swift action:

1. Gather all related documentation and write a description of the situation.
2. Bring all pertinent information to the attention of the General Counsel, the Director of Public Safety, the Chief Financial Officer, the Assistant Vice President, Enrollment Student Services and Director of Financial Aid, or the Registrar.

Once reported to the appropriate authority the next steps are:

3. Investigation of the red flag to determine if there has been a breach.
4. Taking additional action when appropriate. This may entail notification of the affected party, changing passwords or implementing other security measures, cooperating with law enforcement, etc.

What is Simmons requiring that I do to Mitigate Red Flag Activity?

In addition to reading this policy and attending relevant University training, it is expected that you have read the University's Information Security Policy regarding actions that may result in impermissible disclosures of insensitive information. This policy gives examples of ways to protect sensitive information, both in hard copy distribution and electronically, such as:

- Refraining from transmitting or sending sensitive information in email;
- Not writing usernames and passwords down or keeping them where others could gain access; and
- Locking all filing cabinets, desk drawers, and any other applicable storage spaces containing sensitive information at the end of each workday or when unsupervised.

Who Will Administer the Program and How Often Will it be Updated?

The Office of the General Counsel and the Chief Financial Officer will be responsible for oversight and administration of this program. The policy will be reviewed on an annual basis to ensure that all aspects of the program are up-to-date in the current business environment. You will be informed of any changes in the program as they occur.

What about Oversight of Service Providers?

Simmons University will collect documents from all vendors, confirming compliance with Red Flag Rules. Such compliance will be part of the annual review of the Red Flag Policy and the General Counsel will ensure that any specific requirements are addressed in any contract between parties, if applicable.

Adopted: March 2011; Amended March 2023