Russell Sage Colleges Financial Information Security Program (GLBA)

OVERVIEW

Federal Trade Commission (FTC) Rules for safeguarding customer information require financial institutions (including colleges and universities) to implement a Financial Information Security Program. These rules stem from the Gramm-Leach Bliley Act (GLBA) which was passed in 2000. It contained specific requirements regarding the privacy of customer financial information and colleges and universities are deemed to be in compliance if they are in compliance with the Family Educational Rights and Privacy Act (FERPA).

The FTC Rules for Safeguarding Customer Information were published in May, 2002 and apply to colleges and universities because they engage in making and servicing loans (Perkins and College loans). These rules require financial institutions (including colleges and universities) to implement a program to ensure the safeguarding of customer information.

OBJECTIVE

- Designate one or more employees to coordinate the safeguards;
- Identify and assess the risks to customer information in each
- relevant area of the company's operations, and evaluate the
- effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor it and test it;
- Select appropriate service providers and contract with them to implement safeguards, and
- Evaluate and adjust the program in light of relevant circumstances.

Responsibility for Coordinating a Financial Information Security Program

Russell Sage College administration has designated the Director of IT and CIO to coordinate a Financial Information Security Program.

Identifying and Assessing Risks to Customer Information

This group identified Russell Sage Colleges customers as its students and their families, donors, and alumni and any other individuals or entities placed into our databases. Customer information is defined in the FTC Rule on Privacy of Consumer Financial Information (16CFR Par 313) as any record that contains nonpublic personal information (NPI). NPI is described as

- personally identifiable financial information; and
- any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

The ruling goes on to state that NPI does not include publicly available information which is information that someone may have a reasonable basis to believe is lawfully made available to the general public. Organizations have a reasonable basis to believe that information is made available to the general public if:

- they have taken steps to determine that the information is of the type
- that is available to the general public and
- provided customers with the opportunity to direct that the information
- not be made available to the general public and
- complied with such directions.

The Student Services section of Russell Sage Colleges Student Handbook describes the college's compliance with FERPA and notifies students that the college has the right to release their "Directory Information." It goes on to describe "Directory Information" and states that students or parents may have this information excluded from the directory if they contact the Office of the Registrar. The college's other customers, alumni and donors

are also given the option of having their information excluded from public listings and directories created by the college.

For these reasons, NPI at Russell Sage College is deemed to be limited to information that is normally private or related to a customer's finances. Examples include social security numbers, credit card numbers, bank account numbers and balances, income information, credit history. Lists of names and other public information may also be considered NPI if inclusion on the list is based on a customer's financial information such as loan recipients, income levels, etc.

Departments with access to Nonpublic Personal Information

Admission, Student Services, and Financial Aid

Several employees need to know customers' social security numbers in order to meet their job responsibilities in areas such as cashiering, student loan administration and collections. This information is stored in some systems and displayed on some screens and reports used by these employees. Several employees need to know customer's payment, financial aid, and loan history in order to meet their job responsibilities in the student accounts area. This information is stored in the student information system and displayed on some screens and reports used by these employees. It is also reflected in bills, letters, and tax documents (1042-S and 1098-T) sent to students and their families.

In order to process financial aid applications and awards, several employees have access to data reported on students FASFA (Free Application for Federal Student Aid) which contains information on the student and family income and net assets. Employees also have access to the students' financial aid history.

Checks received in the Student Services Office display bank account information and are deposited to the bank as soon as possible.

Finance and Business Services and Human Resources, (including Payroll)

Some employees have access to customers' bank account numbers in order to meet their job responsibilities in areas such as payroll and cash collection. Bank account information required for the college to pay students receiving wages or stipends via direct deposit is stored in the Colleague system and displayed on some screens and reports used by employees in the Office of Finance and Business Services and Payroll

Some employees need to know customers' salary information in order to meet their job responsibilities in the payroll area. This information is stored in the payroll system and displayed on some screens and reports used by these employees. It is also reflected in tax documents (W-2s, W-4s, 1099s, etc.) sent to employees and government agencies.

Institutional Advancement

In order to collect, deposit, and account for gifts, the Institutional Advancement has access to information received by phone or mail which contains bank account and credit card information.

In order to effectively solicit and report gifts, many employees in Advancement have access to donor information which identifies their income level and giving history. Many donors also provide account information to Advancement employees when discussing gifts to the college.

Management Information Systems

Employees in the programming and support areas have access to data stored in the various systems, much of which is considered customer nonpublic financial information.

Institutional Research

Employees have electronic access to several databases which contain customers' private financial information. Some of this information may be downloaded to these employees' hard drives for warehousing and reporting purposes.

Student Life

Employees in Athletics and Recreation, Career Services, Student Development, the Wellness Center and other areas of Campus Life take checks and process confidential NPI from time to time and need to be included in this policy statement.

Libraries

Library workers can see social security numbers in some of the various library databases and have access to credit card information if customers pay their bills in this fashion.

Safeguards to Control Identified Risks

The risks that any of this nonpublic personal information may be used in an unauthorized manner include the following:

a. Employees with access to this information may use it in an unauthorized manner.
b. Other individuals may inappropriately obtain the information and use it in an unauthorized manner.
c. The college may provide this information to service providers that have not taken appropriate safeguards and the information is used in an unauthorized manner.

The college will implement the following procedures for the purpose of safeguarding the nonpublic financial information of its customers.

Risk A: Employees with access to this information may use it in an unauthorized manner.

Safeguards include

- Carefully check references prior to hiring employees who will have access to customer information.
- Request that employees sign an agreement to follow the college's confidentiality and security standards for handling customer information. Require volunteers to sign an agreement.
- Limit access to customer information to those employees and volunteers who have a business reason for seeing it.
- Require multi-factor authentication for all accounts accessing this information
- Enforce and impose disciplinary measures for any breaches.

Risk B: Other individuals may inappropriately obtain the information and use it in an unauthorized manner.

Safeguards include:

- Communicate to employees and volunteers the importance of safeguarding this customer financial information (via confidentially agreement, training, posted notices). Practices such as sharing passwords, posting passwords near the computer, and logging on to a system for someone else should be discontinued.
- Communicate to customers our commitment to safeguard their financial information. For example, include information on this program in the student handbook and the college's website and caution customers against transmitting confidential data via e-mail.
- Control access to this information so that it is only available to employees that actually require it to do their jobs. Steps to control access include
    - Adequately secure documents and reports in locked cabinets and rooms.

    - Ensure access to physical space where such information is stored is limited to appropriate employees.
    - Caution customers against transmitting confidential data, like account numbers, via electronic mail.
    - Display information on reports and screens only as needed.
    - Implement automatic system logouts after specific period of inactivity.
    - Require multi-factor authentication for all accounts accessing this information
    - Fully encrypt all transfers of data.
- Implement measures to prevent and respond to unauthorized system intrusions. These include the following.
    - Maintain adequate firewalls to fully protect the college's internal network.
    - Regularly run anti-viral software on all systems
    - Grant external access only via VPN (Virtual Private Network).
- Dispose of outdated customer information promptly and in a secure manner. Such measures include the following.
    - Shred documents and reports containing such information that are no longer required for business purposes.
    - Delete emails containing such information as soon as possible.
    - Reformat storage devices such as diskettes and CD's containing private financial information before disposal.
    - Delete all information from any hardware storage device before retiring or transferring machines.

Risk C: The College may provide this information to service providers that have not taken appropriate safeguards and the information is used in an unauthorized manner.

Safeguards include

- Limit authorization for such contracts to the Vice President of Finance and Administration
- Before entering contractual relationship, inquire about the service provider's compliance program with the FTC Ruling for Safeguarding Financial Information. Review supporting documentation.

Contractually require service providers to implement and maintain such safeguards. Below is a recommended addendum to such contracts:

> "In order to provide specific services for Russell Sage College and its constituents, certain customer financial information may be forwarded to your organization as an outside service provider. This information can only be used for the purpose of providing the contracted services. Your organization must meet the standards of the Federal Trade Commission Rule for Safeguarding Customer Information (16 CFR Part 314). Any subcontractors used by your organization which may receive customer financial information pertaining to Russell Sage College must also meet these requirements. Upon request, your organization must provide Russell Sage College with the results of any audits and testing of your organization's safeguards."

Monitoring and Testing

The employees designated to coordinate this program are responsible for regularly monitoring the safeguards within their respective divisions to ensure adequacy and compliance. These employees will meet at least annually to review the following

- how these safeguards have been monitored in their areas and what the findings were,
- new or changed business practices that may require modifications to these safeguards,
- any other issues relevant to the safeguarding of customer nonpublic financial information.

Updated- February 23, 2024

Updated-September 15, 2025