

# GLBA and PCI DSS Compliance

John Milligan

Bursar Operations

April 9, 2024



# What is GLBA?

- Gramm-Leach-Bliley Act (1999)
- Federal law implemented by Federal Trade Commission applicable to “financial institutions”
- Recipient of Title IV Federal Student Aid (FSA)
- Ensures the security and confidentiality of non-public personal information of customers
- Two components:
  - I. Privacy Rule – satisfied by compliance with Family Educational Rights to Privacy Act (FERPA)
  - II. Safeguards Rule

# Safeguards Rule

- Designate employees to coordinate information security program
- Inventory of people, processes, and technologies that store, transmit, or process GLBA-related data and/or personally identifiable information
- Monitor and maintain a safeguards program
- Identify and assess risks to “customer” information
- Monitor mandatory annual employee training
- Maintain an Incident Response Plan

# Ongoing GLBA Activities

- Risk assessment planning
- Continuing documentation of data elements and GLBA scope
- Monitor focus areas within GLBA scope
  - I. Financial Aid
  - II. Bursar Operations
  - III. ITS
- Mandatory annual GLBA training

# What is PCI DSS?

- Payment Card Industry Data Security Standard
- PCI Security Standards Council
  - Founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.
  - Develops and maintains standards
  - Current Standard: PCI DSS Version 4.0
- PCI DSS compliance monitored and validated by payment brand, acquirer, or other entity.
  - Self-Assessment Questionnaire (SAQ)
  - Attestation of Compliance (AOC)

# PCI DSS Goals

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

# LSU's PCI DSS Requirements

- In-Person Card Payment: P2PE or Equivalent
- Online Card Payment: SAQ A Payment Solution
- Review of Third-Party Service Providers for PCI DSS Compliance
- Mandatory Annual PCI DSS Training

## **GLBA Webpage**

<https://lsu.edu/administration/ofa/oas/bur/glba/glbainfo.php>

## **GLBA Committee Charter**

[https://lsu.edu/administration/ofa/oas/bur/glba/lsu\\_glba\\_committee\\_charter.pdf](https://lsu.edu/administration/ofa/oas/bur/glba/lsu_glba_committee_charter.pdf)



