# GLBA Safeguards Rule for FinTech: Security Program Implementation Guide

Compliance Guide for Financial Technology

Prepared by Jacobian Engineering

Updated: 2026-02-09

This document is for educational purposes and does not constitute legal advice.

## Executive Summary

GLBA refers to the Gramm-Leach-Bliley Act and the safeguards expected for customer information in the financial sector. Even if your organization is not a traditional bank, GLBA-related requirements can apply through your business model, your regulators, or your partners. The outcome is the same. You need a security program that protects nonpublic personal information and that can be explained and defended.

This guide focuses on the Safeguards Rule expectations that show up in FinTech security programs. It explains how to build an information security program, how to manage service providers, and how to produce evidence that regulators and partners expect to see.

---

## GLBA and the Safeguards Rule in plain language

GLBA is a U.S. law that addresses how financial institutions handle customer information. For many FinTech organizations, the practical compliance work is driven by the Safeguards Rule. The rule requires covered entities to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards.

The Safeguards Rule is flexible by design. It does not prescribe a single technology stack. It expects you to understand your risks, implement safeguards, and monitor those safeguards over time. That is why many organizations treat it like a security program blueprint rather than a checklist.

### Who should care about GLBA Safeguards

- **Non-bank financial institutions:** Many lenders, brokers, and financial service providers fall under GLBA coverage.
- **FinTech vendors handling customer data:** Even when a partner is the covered entity, contracts often require similar safeguards.
- **Organizations with bank partnerships:** Banks frequently flow down safeguard expectations through vendor risk programs.
- **Teams expanding internationally:** GLBA can coexist with other privacy laws, which increases the need for clear data governance.

## A note on breach notification requirements

In addition to security program requirements, the Safeguards Rule includes breach notification expectations. The FTC has issued amendments that require notification to the FTC within 30 days of discovering certain security incidents that involve the information of 500 or more consumers.

Treat this as a program requirement, not an afterthought. Incident response and reporting should be designed before an incident occurs.

## Core program elements that auditors and partners look for

A GLBA-aligned security program is easiest to manage when it is built around repeatable elements. Each element should have an owner, a policy, and a way to prove it operates.

### Qualified oversight and accountability

Assign a qualified individual to oversee the information security program and establish reporting to leadership. The program needs a clear owner who can make decisions and track progress.

Define responsibilities, create a security governance cadence, and produce regular reports that cover risk, incidents, and program maturity.

- **Evidence to keep:** Security program charter, Leadership reporting deck, Meeting minutes and action items, Defined roles and responsibilities

### Risk assessment that drives safeguards

GLBA expects you to assess risks to customer information and to use the results to shape your safeguards. A generic assessment that never changes is rarely persuasive.

Inventory where customer information lives, evaluate threats and vulnerabilities, and translate findings into a remediation plan with owners and deadlines.

- **Evidence to keep:** Risk assessment report, Asset and data inventory, Risk register with remediation tracking, Annual review records

### Access control and identity management

Customer information should only be accessible to people who need it. Strong authentication and least privilege reduce the chance of unauthorized access and insider misuse.

Centralize identity, enforce MFA, use role-based access, and run periodic access reviews for sensitive systems.

- **Evidence to keep:** MFA enforcement settings, Access request and approval tickets, Quarterly access review sign-offs, Privileged access audit logs

### Encryption and secure data handling

Encryption protects customer information if systems are compromised or devices are lost. It is also a clear signal of baseline hygiene in partner reviews.

Encrypt sensitive data in transit and at rest where appropriate, manage keys securely, and define rules for where customer information is allowed to be stored.

- **Evidence to keep:** Encryption configuration evidence, Key management procedures, Data handling policy, Storage and retention configurations

## Secure development and change management

Many FinTech incidents start with application weaknesses and misconfigurations. GLBA-aligned programs expect secure development practices and controlled changes to production systems.

Use code review, dependency scanning, environment separation, and change approvals. Track production changes through tickets and maintain deployment logs.

- **Evidence to keep:** Pull request review records, CI/CD logs, Change tickets and approvals, Secure development policy

## Monitoring, detection, and incident response

You need the ability to detect security events, respond, and learn from incidents. A plan that is never tested does not hold up well in reviews.

Centralize logs, define alerting, run incident response exercises, and document how incidents are triaged and resolved.

- **Evidence to keep:** Log retention settings, Alerting rules and runbooks, Incident tickets and post-incident reviews, Tabletop exercise results

## Service provider oversight

FinTech stacks depend on third parties, including cloud providers, data processors, and outsourced support. GLBA expects you to select and oversee service providers that can access customer information.

Define vendor security requirements, review SOC reports or assessments, and monitor key vendors on a schedule. Make sure contracts include security expectations and incident communication terms.

- **Evidence to keep:** Vendor inventory and tiering, Vendor risk assessment records, Contract security clauses, SOC reports and review notes

### Testing, continuous improvement, and training

The Safeguards Rule expects ongoing evaluation of your controls. Training is a recurring theme because people are part of the security boundary.

Run vulnerability scans, penetration tests, and periodic program reviews. Train staff on data handling, phishing, and incident reporting expectations.

- **Evidence to keep:** Vulnerability scan reports, Penetration test reports and remediation tracking, Security awareness training completion records, Annual program review results

## Data governance and retention for customer information

GLBA-aligned safeguards are easier to implement when you know what data you have and why you have it. Many organizations retain more customer information than they need, which increases breach impact and compliance work.

### Practical steps that reduce exposure

- **Define a data classification scheme:** At minimum, distinguish public data, internal data, and customer information with restricted handling rules.
- **Minimize data collection:** Collect only what is needed for the product and avoid copying sensitive data into analytics and support tooling.
- **Set retention periods:** Define how long customer information is kept and automate deletion where possible.
- **Control exports:** Limit bulk exports and monitor for unusual downloads of customer information.
- **Audit where data travels:** Map data movement to vendors, backups, logs, and developer tooling.

## Third-party contracts and shared responsibility

Service provider oversight is not only a questionnaire exercise. Contracts should reflect how incidents are handled, how data is protected, and what happens when a vendor fails to meet expectations.

### Contract clauses that reduce risk

- **Security requirements:** Minimum access control, encryption, logging, and vulnerability management expectations.

- **Incident notification:** Clear timelines and points of contact for security incidents and breaches.
- **Audit and evidence rights:** The ability to receive SOC reports or equivalent evidence on a schedule.
- **Sub-processor control:** Approval requirements for new sub-processors that touch customer information.
- **Termination and data return:** Secure data deletion or return procedures at the end of a contract.

## Implementation methodology for GLBA Safeguards

### Phase 1: Assess and define the program

Confirm whether GLBA Safeguards applies directly to your organization and identify where customer information is stored and processed. Produce a risk assessment, define program ownership, and set a compliance calendar.

### Phase 2: Implement safeguards and documentation

Implement the safeguards that reduce the highest risks first. Build policies and procedures that reflect reality, not wishful thinking. Align vendor management and incident response with your business model.

### Phase 3: Operate, test, and improve

Move into steady-state operation with regular scans, testing, access reviews, vendor reviews, and incident response exercises. Track findings to closure and document improvements.

## How Jacobian Engineering supports GLBA-aligned programs

GLBA Safeguards work sits at the intersection of security, risk, and operational maturity. Jacobian Engineering supports FinTech teams that need practical implementation.

- **Security program design:** Risk assessments, policy writing, and right-sized program governance.
- **Cloud and application security implementation:** Logging, access control, encryption configuration, and secure delivery practices.
- **Vendor risk management:** Vendor tiering, SOC report reviews, and third-party security requirements.

- **Incident response readiness:** Runbooks, tabletop exercises, and post-incident improvement planning.
- **Ongoing monitoring:** Compliance calendar management and continuous evidence routines.

## Business benefits

A GLBA-aligned program is not only about satisfying a regulator. It also improves day-to-day security outcomes.

- **Lower customer information risk:** Stronger access control, monitoring, and encryption reduce exposure.
- **Faster bank partner onboarding:** A clear security program and vendor oversight process reduces friction in partner reviews.
- **Reduced incident impact:** Prepared incident response and clear data inventories improve containment and recovery.
- **Better operational discipline:** Documented procedures and steady-state routines reduce surprises.

## FAQs

### Does GLBA apply to every FinTech company?

Coverage depends on what services you provide and how regulators classify your organization. Even when you are not directly covered, bank partners and enterprise customers often require similar safeguards through contracts.

### What is nonpublic personal information (NPI)?

NPI generally refers to personal financial information that is not publicly available and that you collect in connection with providing a financial product or service. Treat it as sensitive data with restricted access and clear retention rules.

### How should we handle breach notification under the Safeguards Rule?

Build incident reporting into your incident response plan. Confirm reporting triggers, define who makes decisions, and practice the process through tabletop exercises so it works under pressure.

### Do SOC 2 reports replace GLBA safeguards?

SOC 2 can support GLBA expectations, but it is not a substitute for GLBA obligations. Partners may accept SOC 2 evidence for parts of the program, but you still need GLBA-aligned

governance, risk assessment, and vendor oversight.

### How often should we review vendors?

Use a tiering approach. High-risk vendors should be reviewed more often, especially if they store or process customer information or support critical business functions.

## Primary references

- FTC guidance on the Safeguards Rule: ftc.gov
- FTC Safeguards Rule notification requirement overview: ftc.gov blog
- FTC overview of GLBA: ftc.gov