Gramm–Leach–Bliley Act (GLBA) — Safeguards & Privacy Requirements

Document ID	NB-69-25
Purpose	Selected GLBA sections related to customer data protection, privacy, and security controls.
Classification	Internal Reference for CTF

1. Key Definitions

Nonpublic Personal Information (NPI) — personally identifiable financial information provided by a consumer to a financial institution.
Customer Information — any record containing NPI handled or maintained by or on behalf of a financial institution.

2. Privacy Rule Requirements (§6802)

- Provide customers with clear and conspicuous privacy notices at the time of establishing a relationship and annually thereafter.
- Disclose categories of information collected, how it is used, and with whom it is shared.
- Provide an opt-out option for sharing data with non-affiliated third parties.
- Contracts with service providers must include clauses protecting customer information.

3. Safeguards Rule Requirements (§314.4)

Financial institutions must develop, implement, and maintain a comprehensive written information security program (WISP). It must include:
1. Risk Assessment — identify reasonably foreseeable internal and external risks.
2. Access Controls — restrict access to customer information to authorized personnel only.
3. Encryption — protect customer information at rest and in transit.
4. Incident Response Plan — procedures for detecting, responding to, and recovering from security events.
5. Employee Training — ensure staff understand responsibilities in safeguarding customer data.
6. Testing & Monitoring — regular testing of key controls and systems.
7. Service Provider Oversight — require service providers to maintain appropriate safeguards.
8. Program Updates — adjust security program in light of changes to risks, business operations, or technology.

4. Administrative Requirements

- Designate a Qualified Individual (QI) responsible for the security program.
- Provide annual reports to the Board of Directors or equivalent governing body on program status, risks, and remediation activities.

5. Enforcement & Penalties

- Regulatory Oversight: Federal Trade Commission (FTC), federal banking agencies, and state regulators.
- Penalties: Institutions can face fines up to $100,000 per violation; officers and directors may face personal liability.
- Civil Liability: Consumers may sue for damages resulting from negligence or willful violation.

6. References for CTF Use

Players should reference this document to answer questions such as:
- What data is considered NPI?
- What must be in a WISP?
- What are encryption and access control requirements?
- Who oversees compliance and what are the penalties?