**GLBA (Gramm-Leach-Bliley Act): what, who, and the 3 pillars**

**What it is:** U.S. federal law that requires “financial institutions” (broadly defined, including many non-banks) to protect **nonpublic personal information (NPI)** about **consumers/customers** and explain how it’s shared. Core implementing rules:

1. **Privacy Rule** – disclosures & opt-outs (FTC: **16 CFR Part 313**; banks follow **Regulation P, 12 CFR Part 1016**). [Legal Information Institute](https://www.law.cornell.edu/cfr/text/16/part-313?utm_source=chatgpt.com)[eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-313?toc=1&utm_source=chatgpt.com)[Federal Register](https://www.federalregister.gov/documents/2021/12/09/2021-25735/privacy-of-consumer-financial-information-rule-under-the-gramm-leach-bliley-act?utm_source=chatgpt.com)
2. **Safeguards Rule** – security program requirements (FTC: **16 CFR Part 314**). [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
3. **Pretexting (anti-social-engineering) Rule** – prohibits obtaining customer info by false pretenses (**15 U.S.C. § 6821**). [Legal Information Institute](https://www.law.cornell.edu/uscode/text/15/6821?utm_source=chatgpt.com)

**Key definitions you’ll cite:**

* **Financial institution (FTC scope):** non-bank entities substantially engaged in financial activities (e.g., lenders, mortgage brokers, servicers, payday lenders, tax prep firms, certain “finders,” etc.). [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* **Consumer vs. Customer:** a **consumer** obtains a financial product/service; a **customer** has a **continuing relationship**. Customers trigger stronger obligations (privacy notices, safeguards). [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* **NPI/Customer information:** any nonpublic personal info handled by/for the institution. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)

**1) Privacy Rule (what you must show customers)**

**Obligations (high level):**

* **Initial privacy notice** at relationship start; **annual notice** thereafter (with a statutory **exception** if you share only under specific exceptions and don’t change practices).
* **Right to opt-out** before sharing NPI with **non-affiliated** third parties (subject to exceptions).
* **Limits on redisclosure/reuse** by recipients; **account number sharing restrictions** for marketing.
* Use of **model privacy form** is strongly encouraged (safe-harbor style). [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-313?toc=1&utm_source=chatgpt.com)[Consumer Financial Protection Bureau+1](https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/privacy-notices/?utm_source=chatgpt.com)

**Bank vs. non-bank supervision:** Banks follow **Reg P** (CFPB/ prudential regulators); most non-banks follow the FTC Privacy Rule. [Consumer Financial Protection Bureau](https://www.consumerfinance.gov/rules-policy/regulations/1016/?utm_source=chatgpt.com)[Federal Trade Commission](https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule?utm_source=chatgpt.com)

**Interview tips (Privacy):**

* Explain **when annual notice is not required** (the FAST Act exception baked into Reg P; no material change; sharing only under exceptions).
* Be ready to map an institution’s **data sharing matrix** to opt-out requirements and exceptions. [Federal Register](https://www.federalregister.gov/documents/2018/08/17/2018-17572/amendment-to-the-annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p?utm_source=chatgpt.com)[FDIC](https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf?utm_source=chatgpt.com)

**2) Safeguards Rule (the security program)**

**Program elements you must evidence** (16 CFR §314.4):

* **Qualified Individual** (QI) designated to run the program; **written** information security program.
* **Written risk assessment** with criteria for risk eval/categorization and CIA impact; periodic updates.
* **Controls:**
  + Access control & least privilege
  + **Asset/data inventory & classification**
  + **Encryption of customer info in transit & at rest** (or QI-approved compensating controls)
  + **MFA** for any information system access (QI may approve equivalent)
  + Secure SDLC for in-house and vetting for third-party apps
  + **Data retention & secure disposal** (generally ≤2 years unless needed/required)
  + Change management
  + **Monitoring & logging** of authorized users
* **Testing/Monitoring:** continuous monitoring **or** at least **annual penetration testing** and **semiannual vulnerability assessments**.
* **Training & staffing** (qualified security personnel).
* **Service provider oversight** (due diligence, contractual security requirements, periodic assessment).
* **Incident response plan** with roles, comms, remediation, documentation, and post-incident review.
* **Board (or senior officer) reporting** **at least annually** on program status, testing, service providers, incidents, and recommendations.
* **Adjust program** as risks/operations change. [eCFR+1](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)

**Breach notification (newer):**

* **Notify the FTC within 30 days** of discovery if a security event **involves 500+ consumers** (Safeguards Rule §314.4(j)). **Effective May 13, 2024**.
* **Definition** of “notification event/security event” is in §314.2/§314.4(j). [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)[Federal Trade Commission](https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect?utm_source=chatgpt.com)

**Small entity carve-outs:** If you maintain customer info on **<5,000 consumers**, some specifics (written risk-assessment detail, pen-test/vuln frequency specifics, incident response plan, and board reporting) **don’t apply**—but you still need a reasonable security program. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)

**3) Pretexting (anti-social-engineering)**

Prohibits obtaining customer info by deception (posing as a customer/employee, etc.). Expect to tie this to **phishing/social engineering** controls and training. [Legal Information Institute](https://www.law.cornell.edu/uscode/text/15/6821?utm_source=chatgpt.com)

**How you’ll run a GLBA compliance program (implementation view)**

1. **Scope & data inventory:** Identify systems, vendors, and processes touching **NPI/customer info**; classify data. (Safeguards Rule) [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
2. **Risk assessment:** Written; cover threats, CIA impact, control sufficiency; define risk treatment. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
3. **Policies & controls:** Access, encryption, MFA, SDLC, logging, retention/disposal, change mgmt. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
4. **Vendor risk mgmt:** Due diligence, contracts with security clauses, ongoing monitoring. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
5. **Privacy notices & opt-outs:** Use Reg P/FTC model forms; ensure processes to honor opt-outs and redisclosure limits. [Consumer Financial Protection Bureau](https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/privacy-notices/model-privacy-form/?utm_source=chatgpt.com)[Legal Information Institute](https://www.law.cornell.edu/cfr/text/16/part-313?utm_source=chatgpt.com)
6. **Training:** Security awareness + role-based, including pretexting scenarios. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
7. **Testing & monitoring:** Continuous monitoring **or** annual pen test + semiannual vuln scans; track findings to closure. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
8. **IR & breach notification:** Tabletop; clarify triggers, content, and **FTC 30-day** timeline. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)[Federal Trade Commission](https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect?utm_source=chatgpt.com)
9. **Governance:** QI in place; **annual Board report**; program updates after changes/incidents. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)

**What auditors will ask you to produce (evidence pack)**

* Charter naming the **Qualified Individual**; org chart; RACI. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* **Written risk assessment** + updates. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* Policies/standards: access control, encryption, MFA, SDLC, logging, vendor mgmt, data retention/disposal, change mgmt. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* **Pen test** & **vuln** reports (and remediation tracking); monitoring outputs. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* **Training** records; phishing simulations addressing pretexting. [Legal Information Institute](https://www.law.cornell.edu/uscode/text/15/6821?utm_source=chatgpt.com)
* **Vendor due diligence** artifacts + contracts with safeguard clauses. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
* **Incident response plan**, tabletop minutes, and any **FTC notification** proof if applicable. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)[Federal Trade Commission](https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect?utm_source=chatgpt.com)
* **Privacy notices** (initial/annual), opt-out logs, redisclosure controls; **model form** usage. [Consumer Financial Protection Bureau](https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/privacy-notices/model-privacy-form/?utm_source=chatgpt.com)
* **Annual Board report** (topics listed in §314.4(i)). [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)

**Interview-style questions (and what a strong answer hits)**

1. **GLBA vs. ISO 27001/NIST CSF:**
   * GLBA is **law + rules** (Privacy & Safeguards); ISO/NIST are **frameworks**. Map Safeguards Rule to NIST CSF (ID, PR, DE, RS, RC) and ISO Annex A families to show alignment. (No citation needed; conceptual mapping.)
2. **When can we skip annual privacy notices?**
   * Only if sharing is **limited to statutory exceptions** and there’s **no material change** in practices since the last notice (FAST Act exception baked into Reg P). [Federal Register](https://www.federalregister.gov/documents/2018/08/17/2018-17572/amendment-to-the-annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p?utm_source=chatgpt.com)
3. **What’s “customer information” and who’s in scope under FTC vs. Reg P?**
   * Define **consumer/customer** precisely; explain **FTC jurisdiction** over non-banks vs **CFPB/banking agencies** over banks. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)[Consumer Financial Protection Bureau](https://www.consumerfinance.gov/rules-policy/regulations/1016/?utm_source=chatgpt.com)
4. **Safeguards must-haves in 2024/2025:**
   * **QI**, **written risk assessment**, **encryption (at rest/in transit)**, **MFA**, **monitoring/logging**, **testing cadence**, **IR plan**, **Board report**, and **FTC 30-day breach notification** for 500+ consumers. [eCFR+1](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
5. **How do you oversee service providers?**
   * Due diligence, contractual safeguards, periodic assessments; include offboarding & incident-notification clauses. [eCFR](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314)
6. **Pretexting controls?**
   * Training + process controls (KBA, call-back, least privilege, help-desk scripts, phishing simulation). [Legal Information Institute](https://www.law.cornell.edu/uscode/text/15/6821?utm_source=chatgpt.com)