FTC Safeguards Checklist
For Financial Institutions

The FTC Safeguards Rule is **now in full effect** — and as of **May 13, 2024**, covered businesses must report qualifying data breaches to the FTC.

PART 1 — Required Policies

- [ ] **Designated Qualified Individual**
  Appoint an individual to oversee your information security program. They must have skills considered adequate for the amount and sensitivity of the data you store.

- [ ] **Incident Response Plan**
  Document the actions your team takes during a cyber incident: preparation, identification, containment, eradication, recovery, and lessons learned.

- [ ] **Information Access Controls, Disposal Plan & Change Management**
  Restrict who can make changes and keep an audit trail of all of them. Change management defines the process when your technology stack changes. A disposal plan governs secure disposal of customer information — the Rule generally requires a two-year limit, with some exceptions.

- [ ] **Oversee Service Providers & App Review**
  Review every vendor with access to your customer information. They must meet these safeguards too — you remain responsible for your data and for the providers who handle it.

Does This Affect Me?

Financial Institution means any business that is financial in nature, or incidental to such financial activities.

EXAMPLES

- Auto dealerships
- Mortgage lenders or brokers
- Payday lenders
- Finance companies
- Tax preparation firms
- Accounting agencies
- Collection agencies
- Financial advisors
- Investment advisors not registered with the SEC

PART 2 — Reports & Documentation

- [ ] **Data & Systems Inventory**
  Maintain an inventory of all the customer data you hold and the systems it lives on — you can't protect what you haven't accounted for.
- [ ] **Risk Assessment**
  Identify internal and external threats to the security, confidentiality, and integrity of customer information. This written assessment must include the criteria you use to evaluate those risks and threats.
- [ ] **Information Security Program**
  This entire checklist forms part of your information security program. Building one is an ongoing process that draws on every area of security described here, and more.
- [ ] **Report to Your Board of Directors**
  Your Qualified Individual must report to your Board of Directors — or a Senior Officer if there is no board — on a regular basis, at least once a year.

PART 3 — Technical Requirements

- [ ] **Multi-Factor Authentication (MFA)**
  Enable MFA on every system employees and contractors log into. It adds a second layer of identity verification and blunts phishing, stolen-credential, and account-takeover attacks.
- [ ] **Data Encryption**
  Encrypt customer information at rest and in transit. Where encryption isn't feasible, use effective alternative controls approved by your Qualified Individual.
- [ ] **Penetration Testing & Vulnerability Assessments**
  Pen testing, vulnerability assessments, and continuous monitoring detect and prevent attacks. Without continuous monitoring, conduct annual pen testing plus vulnerability assessments, including system-wide scans every six months for publicly-known vulnerabilities.
- [ ] **Monitor & Log Activity**
  Implement a solution that logs when authorized users access customer information and detects unauthorized or suspicious access.

PART 4 — Training Requirements

- [ ] **Employee Security Awareness Training**
  Give your people security awareness training, and schedule regular refreshers.
- [ ] **Training & Updates for Security Personnel**
  Provide specialized training for staff and providers who are hands-on with your security program, and verify they stay current on emerging threats and countermeasures.

NEW · Effective May 13, 2024

Report Notification Events to the FTC

If you discover a **notification event** — the unauthorized acquisition of unencrypted customer information affecting **500 or more consumers** — you must notify the FTC **as soon as possible, and no later than 30 days** after discovery, using the FTC's online reporting form. Review your incident response plan and vendor contracts so you can report within the deadline.

Not sure where your business stands?

eMDTec helps small and mid-sized businesses across NJ, NY & PA build and maintain FTC Safeguards-compliant security programs — assessment, implementation, and ongoing management.

Assess
Gap assessment against every item on this checklist, with a prioritized roadmap.

Implement
MFA, encryption, monitoring, access controls, and documented policies — managed for you.

Sustain
Ongoing monitoring, training, testing, and annual reporting to keep you compliant.

Book a free consultation

john.emdtec.com

155 Pompton Ave, STE 107, Verona, NJ 07044 • 973-295-5570 • Support 973-295-9500

This checklist summarizes key requirements of the FTC Standards for Safeguarding Customer Information (16 C.F.R. Part 314) for general guidance and is not legal advice. Consult the full Rule and qualified counsel for your specific obligations.