2025 FTC Safeguards Rule Compliance Checklist

Complete Compliance Verification Guide for Financial Institutions

---

RebootTwice LLC
FTC Compliance Experts
Phone: (949) 831-8821
Email: sales@reboottwice.com
Web: www.reboottwice.com

Last Updated: January 2025
Version: 2.0
Penalty Risk: Up to $51,744 per violation

Page 1: Core Requirements & Risk Assessment

✅ FUNDAMENTAL COMPLIANCE REQUIREMENTS

1. Written Information Security Program (WISP)

- ☐ **WISP document created and implemented** *(Required for all covered entities)*
- ☐ **WISP covers all required elements** *(See detailed checklist on Page 2)*
- ☐ **WISP reviewed and updated annually** *(Must document review process)*
- ☐ **WISP accessible to relevant staff** *(Proper distribution and training)*
- ☐ **Board or senior leadership approval documented** *(Required oversight)*

2. Designated Qualified Individual

- ☐ **Qualified Individual formally designated** *(Must have cybersecurity expertise)*
- ☐ **Individual has authority to implement program** *(Clear organizational authority)*
- ☐ **Ongoing training and certification maintained** *(Stay current with threats)*
- ☐ **Regular reporting to board/leadership established** *(Documented communication)*

3. Risk Assessment (Annual Requirement)

- ☐ **Current risk assessment completed within 12 months**
- ☐ **Assessment covers all data systems and processes**
- ☐ **Third-party vendor risks evaluated**
- ☐ **Remote access risks documented**
- ☐ **Physical security risks assessed**
- ☐ **Risk mitigation plan developed**
- ☐ **High-risk areas prioritized for immediate action**

4. Small Entity Exemption Verification

- ☐ **Customer record count verified** *(Under 5,000 = potential exemption)*
- ☐ **Exemption eligibility documented** *(Annual verification required)*
- ☐ **Basic safeguards still implemented** *(Even if exempt from full rule)*

🚨 IMMEDIATE ACTION ITEMS *(High Penalty Risk)*

Multi-Factor Authentication (MFA) - MANDATORY

- [ ] **MFA implemented for ALL systems with customer data**
- [ ] **MFA covers email accounts** *(Major enforcement focus)*
- [ ] **MFA for administrative accounts** *(System admin access)*
- [ ] **MFA for remote access** *(VPN, cloud systems)*
- [ ] **MFA bypass procedures documented** *(Emergency access only)*

Encryption Requirements

- [ ] **Customer data encrypted at rest** *(Database, file storage)*
- [ ] **Customer data encrypted in transit** *(Email, web transfers)*
- [ ] **Mobile device encryption enabled** *(Laptops, phones, tablets)*
- [ ] **Encryption key management documented** *(Secure key storage)*

Access Controls

- [ ] **User access regularly reviewed** *(Quarterly minimum)*
- [ ] **Terminated employee access immediately revoked**
- [ ] **Least privilege principle implemented** *(Minimum necessary access)*
- [ ] **Admin privileges limited and monitored** *(Elevated access tracking)*

📊 INDUSTRY-SPECIFIC CONSIDERATIONS

Tax Preparation Services

- [ ] **IRS Publication 4557 alignment verified**
- [ ] **E-filing security requirements met**
- [ ] **PTIN holder data protection implemented**
- [ ] **Seasonal staff security procedures established**

Check Cashing & Money Services

- [ ] **Bank Secrecy Act (BSA) integration completed**
- [ ] **FinCEN reporting system security verified**
- [ ] **Cash handling procedures documented**
- [ ] **Multi-location security standardized**

Mortgage & Real Estate Finance

- [ ] **CFPB requirements integrated**
- [ ] **TRID compliance data protection verified**
- [ ] **NMLS system security implemented**
- [ ] **Loan file encryption confirmed**

Investment Advisors

- [ ] **SEC Form ADV cybersecurity disclosure updated**
- [ ] **Client portal security verified**

- [ ] **Portfolio data encryption confirmed**
- [ ] **Fiduciary data obligations documented**

Page 2: Detailed WISP Requirements

✅ REQUIRED WISP ELEMENTS *(All Must Be Documented)*

Administrative Safeguards

- [ ] **Security Officer designated with contact information**
- [ ] **Employee security training program established**
- [ ] **Background check procedures documented**
- [ ] **Disciplinary measures for security violations defined**
- [ ] **Regular security awareness communications scheduled**

Physical Safeguards

- [ ] **Facility access controls implemented** *(Locks, badges, monitoring)*
- [ ] **Computer workstation security controls** *(Screen locks, positioning)*
- [ ] **Media controls and disposal procedures** *(Secure destruction)*
- [ ] **Equipment inventory and tracking system**

Technical Safeguards

- [ ] **Access control systems implemented** *(User authentication)*
- [ ] **Audit controls and monitoring established** *(Log review procedures)*
- [ ] **Data integrity controls implemented** *(Backup and recovery)*
- [ ] **Transmission security protocols established** *(Encrypted communications)*

Vendor Management Program

- [ ] **Service provider security assessments required**
- [ ] **Contractual security requirements included**
- [ ] **Due diligence procedures documented**
- [ ] **Ongoing vendor monitoring established**
- [ ] **Contract terms include data security provisions**

🔄 ONGOING MONITORING & TESTING

Continuous Monitoring Requirements

- [ ] **Authorized user activity monitoring** *(User behavior analytics)*
- [ ] **Data access logging and review** *(Who accessed what, when)*
- [ ] **System change management procedures** *(Documented approval process)*
- [ ] **Vulnerability scanning scheduled** *(Regular security assessments)*

Penetration Testing & Assessments

- [ ] **Annual penetration testing scheduled** *(External security assessment)*
- [ ] **Vulnerability assessments conducted quarterly**
- [ ] **Social engineering testing included** *(Email phishing simulation)*

- [ ] **Physical security testing performed** *(Access control verification)*

Response & Recovery Planning

- [ ] **Incident response plan documented** *(Step-by-step procedures)*
- [ ] **Response team members identified** *(Contact information current)*
- [ ] **Communication procedures established** *(Internal and external)*
- [ ] **Recovery procedures tested annually** *(Documented testing results)*

📱 REMOTE WORK & MOBILE DEVICE SECURITY

Remote Access Controls

- [ ] **VPN security requirements established**
- [ ] **Home office security guidelines provided**
- [ ] **Personal device usage policies defined** *(BYOD security)*
- [ ] **Cloud service usage restrictions documented**

Mobile Device Management

- [ ] **Device encryption requirements enforced**
- [ ] **Remote wipe capabilities implemented**
- [ ] **App installation restrictions defined**
- [ ] **Lost/stolen device procedures established**

🔐 DATA CLASSIFICATION & HANDLING

Customer Information Protection

- [ ] **Data classification system implemented** *(Public, internal, confidential)*
- [ ] **Handling procedures for each classification level**
- [ ] **Retention schedules documented** *(How long to keep data)*
- [ ] **Secure disposal procedures established** *(Data destruction methods)*

Information Sharing Controls

- [ ] **Need-to-know access principles applied**
- [ ] **External sharing approval procedures**
- [ ] **Third-party disclosure tracking** *(Who has access to what)*
- [ ] **Data location restrictions documented** *(Geographic limitations)*

Page 3: Breach Response & Reporting

🚨 INCIDENT RESPONSE REQUIREMENTS

Immediate Response (First 24 Hours)

- [ ] **Incident detection procedures established** *(How breaches are identified)*
- [ ] **Response team activation process documented**
- [ ] **Containment procedures implemented** *(Stop ongoing breach)*

- [ ] **Evidence preservation procedures defined** *(Forensic considerations)*
- [ ] **Initial impact assessment conducted** *(Scope and severity)*

Investigation & Assessment (Days 1-7)

- [ ] **Forensic investigation procedures established**
- [ ] **Root cause analysis requirements documented**
- [ ] **Affected customer identification process**
- [ ] **Risk assessment methodology defined**
- [ ] **Legal counsel notification procedures**

Notification & Reporting (Within 30 Days)

- [ ] **FTC notification requirements understood** *(Security Event Form)*
- [ ] **State attorney general notification procedures**
- [ ] **Customer notification templates prepared**
- [ ] **Media response procedures documented**
- [ ] **Regulatory agency contact information current**

📋 FTC SECURITY EVENT REPORTING

Reporting Threshold (500+ Consumers)

- [ ] **Consumer count tracking system implemented**
- [ ] **Reporting timeline understood** *(Within 30 days of discovery)*
- [ ] **Required information compilation process** *(What data to include)*
- [ ] **Form submission procedures documented**

Required Reporting Information

- [ ] **Incident description template prepared**
- [ ] **Consumer impact assessment procedures**
- [ ] **Remediation action documentation process**
- [ ] **Timeline reconstruction capabilities**
- [ ] **Contact information for regulatory follow-up**

🔧 POST-INCIDENT ACTIVITIES

Remediation & Recovery

- [ ] **System restoration procedures documented**
- [ ] **Security enhancement identification process**
- [ ] **Customer communication follow-up procedures**
- [ ] **Business continuity plan activation**

Lessons Learned & Improvement

- [ ] **Post-incident review procedures established**
- [ ] **WISP update process based on incidents**
- [ ] **Training program updates based on lessons learned**

- [ ] **Third-party assessment consideration process**

👥 EMPLOYEE TRAINING & AWARENESS

Mandatory Training Topics

- [ ] **Password security and MFA usage**
- [ ] **Phishing and social engineering recognition**
- [ ] **Physical security awareness**
- [ ] **Incident reporting procedures**
- [ ] **Data handling and protection requirements**

Training Documentation

- [ ] **Attendance records maintained** *(Who attended when)*
- [ ] **Competency testing implemented** *(Verify understanding)*
- [ ] **Refresher training scheduled** *(Annual minimum)*
- [ ] **Role-specific training provided** *(Different levels for different roles)*

New Employee Onboarding

- [ ] **Security orientation within first week**
- [ ] **Account setup security procedures**
- [ ] **System access training completed**
- [ ] **Security policy acknowledgment signed**

🏢 BOARD & EXECUTIVE OVERSIGHT

Governance Requirements

- [ ] **Board cybersecurity expertise verified** *(Qualified individual or advisor)*
- [ ] **Regular reporting schedule established** *(Quarterly minimum)*
- [ ] **Budget allocation for security improvements**
- [ ] **Executive accountability measures defined**

Reporting & Documentation

- [ ] **Risk assessment summaries for board review**
- [ ] **Incident reporting to board procedures**
- [ ] **Compliance status reporting format established**
- [ ] **Investment in security infrastructure documented**

Page 4: Implementation Timeline & Verification

🗓️ 90-DAY IMPLEMENTATION ROADMAP

Days 1-30: Foundation & Assessment

- [ ] **Week 1:** Designate Qualified Individual and form security team
- [ ] **Week 2:** Conduct comprehensive risk assessment

- [ ] **Week 3:** Implement immediate MFA requirements
- [ ] **Week 4:** Draft initial WISP document outline

Days 31-60: Core Implementation

- [ ] **Week 5-6:** Complete WISP documentation
- [ ] **Week 7:** Implement encryption requirements
- [ ] **Week 8:** Establish access control procedures

Days 61-90: Testing & Finalization

- [ ] **Week 9:** Conduct security testing and validation
- [ ] **Week 10:** Complete employee training program
- [ ] **Week 11:** Final WISP review and board approval
- [ ] **Week 12:** Document compliance and prepare for audit**

✅ VERIFICATION & AUDIT CHECKLIST

Documentation Verification

- [ ] **All required policies documented and current**
- [ ] **Employee training records complete and up-to-date**
- [ ] **Vendor agreements include required security terms**
- [ ] **Incident response procedures tested and documented**
- [ ] **Board oversight activities documented**

Technical Verification

- [ ] **MFA functioning on all required systems**
- [ ] **Encryption properly implemented and tested**
- [ ] **Access controls working as designed**
- [ ] **Monitoring systems operational and reviewed**
- [ ] **Backup and recovery procedures tested**

Compliance Verification

- [ ] **Risk assessment completed within last 12 months**
- [ ] **Security testing conducted and documented**
- [ ] **Employee training current for all staff**
- [ ] **Vendor assessments completed**
- [ ] **Incident response plan tested**

🎯 ONGOING COMPLIANCE MAINTENANCE

Monthly Activities

- [ ] **Review access control reports**
- [ ] **Update security awareness communications**
- [ ] **Review vendor security status**
- [ ] **Monitor security tool effectiveness**

Quarterly Activities

- [ ] **Conduct vulnerability assessments**
- [ ] **Review and update employee access**
- [ ] **Test incident response procedures**
- [ ] **Report to board/senior leadership**

Annual Activities

- [ ] **Complete comprehensive risk assessment**
- [ ] **Update WISP based on risk assessment**
- [ ] **Conduct penetration testing**
- [ ] **Review and update all security policies**
- [ ] **Evaluate Qualified Individual effectiveness**

📞 NEED HELP WITH COMPLIANCE?

RebootTwice Expert Services

- **Free Compliance Assessment:** Identify gaps and priorities
- **WISP Development:** Industry-specific documentation
- **Implementation Support:** 30-day delivery guarantee
- **Ongoing Maintenance:** Monthly compliance monitoring

Contact Information

Phone: (949) 831-8821
Email: sales@reboottwice.com
Website: www.reboottwice.com

Our Credentials

- **CISSP & CISM Certified Experts**
- **30+ Years Compliance Experience**
- **100% Client Success Rate**
- **$0 Client Penalties to Date**

⚠️ IMPORTANT DISCLAIMERS

This checklist is for informational purposes only and does not constitute legal advice. FTC requirements may change, and specific circumstances may require additional measures. Consult with qualified cybersecurity and legal professionals for comprehensive compliance guidance.

Penalty amounts and requirements are based on 2025 FTC guidelines and may be updated. Always refer to current FTC publications for the most recent requirements.

Version 2.0 - January 2025