Blumira

FTC Safeguards Checklist For Financial Institutions

FTC Safeguard Rules are going into effect on December 9, 2022.
Have you checked off all the boxes?

Part 1: Required Policies

☐ Designated Qualified Individual

An individual on the IT/security team who oversees the security program. They must have skills that are considered "adequate" for the amount of data you're storing.

Options:

- Current employee with the qualifications (or with training)
- Service providers can assist, but internal person is ultimately responsible

☐ Incident Response Plan

This plan details a series of actions that the security team must take in the event of a cyber incident: preparation; identification; containment, eradication; recovery; and lessons learned.

Options:

- Hire an incident response firm to help
- Develop an incident response plan internally (example)

Dynamic blocklists are an excellent example of a network-based containment technology. Blumira supports several next-gen firewalls that you can configure to perform this containment step automatically.

☑ Information Access Controls, Disposal Plan & Change Management

Information access controls restrict who can make changes and creates an audit trail of all changes.
Change management details what process you should follow when your technology stack changes.
A **disposal plan** lays out the process for secure disposal of customer information. The Safeguards Rule requires a limit of two years — with some exceptions.

Options:

- Request help from your service provider and ensure all of these requirements are being met
- Hire an experienced security consultant to help create them

☐ Oversee Service Providers & Apps

Review your vendors that have access to your customer information. They too must comply with all of these safeguards. Remember, you're responsible for your data and your service providers who handle it.

Options:

- Research and select vendors with standards-based information security programs or certifications like SOC2

Tips: Share this checklist with your vendors and keep it handy for future vendor discussions. Make sure they're aware these safeguards apply to them.

Does This Affect Me?

Financial institution means any institution that is financial in nature or incidental to such financial activities

Examples

- Auto dealerships
- Mortgage lenders or brokers
- Tax preparation firms
- Payday lenders
- Finance companies
- Check cashers or wire transferors
- Collection agencies
- Credit counselors
- Financial advisors

How Blumira Can Help

Blumira can automate this process by reducing the time necessary to conduct access reviews and directing your attention to access events that matter

FTC Safeguards Checklist For Financial Institutions

Part 2: Reports and Documentation

How Blumira Can Help

Using our saved report, "Blumira Summary: Parsed Source Types And Log Counts" you can export a list of all devices sending logs to Blumira.

☐ Data and Systems Inventory

Just like you have to track the cars on your lots, the FTC requires you have an inventory of all data you have stored and the systems they're on.

Options:

- Ask your service provider, they should already have an asset inventory
- Find a software solution that track IT assets and detect new ones

Tips:

Check out the CIS Critical Security Controls SME Companion Guide for best practices developed by IT experts

☐ Risk Assessment

This involves identifying threats to an environment — both internal and external — to the security, confidentiality, and integrity of customer information. This written assessment must include criteria for evaluating those risks and threats.

Options:

- Start with free tools like SimpleRisk and CISAs CSET tool
- Hire a professional risk assessment consultant

Prepare Yourself

While it doesn't replace a professional Risk Assessment, you can use our free threat assessment guide to prepare for the real thing.

☐ Information Security Program

Really, this whole checklist is part of your information security program. Developing one is an ongoing process that requires an understanding of the different facets of security described here, and more.

Options:

- Create it in-house
- Collaborate with a security service provider

Tips:

When building a security program, it's best to work with experts who have experience creating them before. Work with a service provider who already safeguards their own data and has helped numerous customers with their security program. Remember: People, Process, Technology, you need all 3 to make a security program successful.

☐ Report To Your Board of Directors

Your Qualified Individual must give an update to your Board of Directors (or a Senior Officer if there isn't a board) on a regular basis — at least once a year.

Tips:

- Match your existing reporting by pulling reports and key insights from the security tools you've already implemented.
- Set up the reports on a standard recurring basis so everyone knows exactly when they are.

FTC Safeguards Checklist For Financial Institutions

Part 3: Technical Requirements

How Blumira Can Help

Blumira sends a finding to notify when a user bypasses or disables MFA, skips enrollment, or has unusual or impossible logins.

☐ Multi-factor Authentication

Enable multi-factor authentication on all systems that employees and contractors log into. MFA is an easy way to add another layer of verification of a user's identity and prevent the success of attacks like phishing, stolen credentials and account takeovers.

Options:

- Ask your service provider to implement
- MFA vendors such as Duo Security, Okta, Microsoft

Tips: Take advantage of built-in features from tools that you already use. For example, if you already run Microsoft 365, take advantage of the ability to enable MFA for free across your environment.

☐ Data Encryption

Encrypt customer information at rest and when it's in transit. If it's not feasible to use encryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

Options:

- Check with vendors to ensure they're encrypting data properly
- Built-in tools like Bitlocker or FileVault or open source tools like Veracrypt

Tips:

- With Blumira, you can review event logs within the safety of our platform, where they are protected by our security controls and encrypted both at rest and in transit.
- Blumira customers can also use the **Report Builder** feature to discover legacy connections to financial and security tools with unencrypted data.

☐ Penetration Testing and Vulnerability Assessments

Penetration testing, vulnerability assessments and continuous monitoring all help to detect and prevent both actual and attempted attacks.

Without **continuous monitoring**, you must conduct annual **penetration testing** and **vulnerability assessments**, including system-wide scans every six months to test publicly-known vulnerabilities.

Options:

- Work with a service provider to implement vulnerability scanning tools from vendors such as Tenable, or Qualys
- Hire a pentesting firm such as 7 Minute Security

Tips:

With Blumira, you can test your SIEM to ensure its readiness against an upcoming pentest.

FTC Safeguards Checklist For Financial Institutions

Part 3 cnt'd: Technical Requirements

☑ Monitor and Log Authorized and Suspicious Activity

Implement a solution to monitor when authorized users are accessing customer information on your system and to detect unauthorized or suspicious access.

Options:

- Blumira (built for small teams), Splunk (built for Enterprise SOCs) or ELK (built for teams with developers)
- Ask your service provider to implement Blumira

Blumira Checks This Box

Built for small teams, Blumira's cloud-based SIEM provides monitoring and logging along with built-in detections and step-by-step response playbooks.

Tips:

Prioritize a SIEM that fits the resources of your team. Traditional SIEMs, while powerful, take a lot of time and expertise to manage. Blumira, on the other hand, is designed for small teams without expertise and does a lot of the heavy lifting for you, making it easy to run with limited resources.

Part 4: Training Requirements

☐ Employee Security Awareness Training

Provide your people with security awareness training and schedule regular refreshers.

Options:

- Outsource to a vendor such as Curricula or KnowBe4
- Ask your service provider to implement

Tips:

Your service provider likely has a solution for this that can be implemented upon request.

☐ Training and Security Updates for Security Personnel

Provide specialized training for employees, affiliates, or service providers who are hands-on with your information security program and verify that they're monitoring the latest word on emerging threats and countermeasures.

Options:

- An outside consultant that specializes in security programs
- Online certification courses

Tips:

This is a great opportunity to promote growth on your team. Helping individuals in leveling up their career is a great way to show support.

How Blumira Helps Check Boxes ☑

Boxes We Fully Check

☑ Monitor and Log Authorized and Suspicious Activity

It's what we do. Built for small teams, Blumira's cloud-based SIEM provides monitoring and logging along with built-in detections and step-by-step response playbooks.

We Help Support

☐ Penetration Testing and Vulnerability Assessments

Blumira detects attacker behavior also used during a penetration test out of the box, without any complex configuration, or weeks of tuning.

☐ Data Encryption

Blumira encrypts the data collected from your systems in transit and at rest within our platform. Additionally, Blumira can help you look for and eliminate legacy protocols in your environment.

☐ Access Controls

Blumira automatically logs user access and when their access levels change to give you insight into your current access activity and controls.

☐ Incident Response Plan

Part of your response plan should include using data and insights from your SIEM (like Blumira) to help figure out what went wrong. Our built-in playbooks provide stacked evidence, which can drastically speed up the incident response process by ensuring that all of the data is in one place.

Why Blumira?

Meet compliance controls, save time on security tasks, focus on real threats and protect against a breach faster than ever with Blumira.

AUTOMATE TASKS FOR YOU

We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts.

FASTER TIME TO SECURITY

Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.

EASILY MEET COMPLIANCE

With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.