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?

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

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.

✓ 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.

✓ Information Access Controls, Disposal Plan & Change Management

Information access controls restrict who can make changes and creates an audit trail of all changes. **Change managemen**t 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.

✓ Oversee Service Providers & Apps

Review your applications you use and vendors that you share data with - if they are also handling customer data, they too must comply with all of these safeguards. And, unfortunately you're on the hook if they're not.

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

Part 2: Reports and Documentation

✓ 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.

✓ Risk Assessment

This involves identifying threats to an environment — both internal and external — to the security, confidentiality, and integrity of customer information.

✓ Information Security Program

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

✓ 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.

FTC Safeguards Checklist For Auto Dealers

Part 3: Technical Requirements

✓ Multi-factor Authentication

Enable multi-factor authentication on all systems that employees and contractors log into.

✓ Penetration Testing and Vulnerability Assessments

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

✓ 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.

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.

Part 4: Training Requirements

✓ Employee Security Awareness Training

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

✓ Training and Security Updates for Security Personnel

Provided 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.

Check The Boxes With 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.