MOSAIC
CYBER SECURITY

Auditing Your Safeguards Program [5 Best Practices]

A Guide to Ensure Your Dealership is Protected, Compliant, and Secure

Have you chosen a Safeguards solution for your dealership? If so, that's a great first step, but your job isn't done yet. As a dealer principal or Qualified Individual, you're responsible for ensuring that your Safeguards Program is not only set up correctly but also effective in protecting customer data. According to the FTC Safeguards Rule, this isn't optional—it's a requirement. But how do you know if your program is actually reducing the risk of data breaches? This whitepaper outlines five essential practices for auditing your Safeguards Program to ensure maximum protection.

Best Practices for Auditing Your Solution

Tip #1 – Use an Audit Worksheet

Regular testing and monitoring are key to fulfilling the Safeguards Rule, which mandates the effectiveness of your safeguard measures. One of the most effective tools for this is an Audit Worksheet. Using a structured worksheet can help you:

- Identify each requirement of the Safeguards Rule
- Review how your dealership's solution meets each requirement
- Record outcomes for future reference

We recommend conducting audits at least annually and using the same worksheet for each audit. Doing so will not only allow you to track your progress but also create a legal record that could be beneficial in court proceedings.

Key Takeaway: Consistency and thorough documentation are your allies in safeguarding your dealership's information systems.

Tip #2 – Complete Your Setup

Relying on a Safeguards solution from an external service provider can simplify compliance, but the accountability for any data breaches or compliance issues ultimately rests with the dealership and the Qualified Individual. Some tasks can only be performed by the dealer or QI. These include, but are not limited to:

- Completing a risk assessment
- Approving service provider attestations
- Ensuring adherence to Safeguard policies

Remember, when it comes to compliance, the FTC holds the dealership and the Qualified Individual accountable, not your safeguards provider.

It's crucial to be proactive in ensuring your store(s) have fully met all Safeguards requirements, for example:

- Have all employees started or completed annual security awareness training?
- Are the new Safeguards policies being implemented?
- Has the executive team reviewed the Annual Safeguard Report?

Avoid the mistake of writing a check and walking away. Compliance is an ongoing process that requires active participation from all stakeholders. See a list of all the requirements here.

Key Takeaway: Neglecting your part in the setup and operation of Safeguards requirements is not just risky—it's a liability. Even with a Safeguards solution in place, there are critical steps that only you can take. Don't overlook them. Your compliance and security depend on it.

Tip #3 – Remediate Risks

When auditing your Safeguards Program, the focus shouldn't only be on identifying risks but also on taking action to close any security gaps. Here are some effective measures:

- **Penetration Tests:** These can offer actionable insights on how to bolster your digital security, based on real-world attempts to infiltrate your network.
- **Vulnerability Scans and Risk Assessments:** Use these tools to identify weak points in your systems.
- **Endpoint Detection and Response:** Implement solutions that continuously monitor and respond to potential threats.

While auditing your Safeguards Program, it's crucial not just to ensure that these risk assessment tools are in place, but also to verify that your dealership is taking active steps to remediate any vulnerabilities uncovered. Doing so could be the difference between secure operations and becoming a cautionary tale. A report from September 14th, 2023, highlighted a stark example:

> "Caesars paid out a ransom worth $15 million to a cybercrime group that managed to infiltrate and disrupt its systems."[1]

Don't let your dealership become another headline.

Key Takeaway: A successful Safeguards Program not only detects threats but also effectively mitigates them. Identifying security risks is just the first step. What counts is how you act on that knowledge.

Tip #4 – Test Your Safeguards

Physical Safeguards: Begin with an unannounced walkthrough of your sales floor. Check for potential risks, such as:

- Deal jackets left open
- Unlocked doors
- Unprotected files

Cyber Safeguards: Leverage a "tabletop" exercise, which simulates a data breach scenario in a controlled environment. This exercise will evaluate the effectiveness of your incident response plan and the readiness of your team.

Policy Check: Make sure your policies reflect actual practices. It's far more beneficial to have a policy that is both accurate and adhered to, rather than one that is 'perfect on paper' but ignored.

Deal Jacket Audits: Regularly auditing your deal jackets can serve as an additional layer of safeguard, helping you to avoid compliance issues and lawsuits that extend beyond the scope of the Safeguards Rule.

Key Takeaway: Testing your safeguards isn't just about ticking off boxes. It's a critical step in confirming that your safeguards are both efficient and effective.

(1) Goswami, R., Brewer, C. (2023, September 14). Caesars paid millions in ransom to cybercrime group prior to MGM hack. CNBC. https://www.cnbc.com/2023/09/14/caesars-paid-millions-in-ransom-to-cybercrime-group-prior-to-mgm-hack.html

Tip #5 – Leverage Resources

Customer Success Teams: If you have a Safeguards Provider, take advantage of their dedicated support staff. Many Qualified Individuals may not specialize in compliance, making these resources invaluable.

Compliance Resources: Compliance providers often have an array of resources at their disposal, ranging from best practices to more hands-on support. Use these resources to ensure optimal protection for your dealership.

Quarterly Check-ins: Once your Safeguards Program is up and running, schedule quarterly meetings to assess risks and adapt your strategy accordingly.

Key Takeaway: Managing compliance can be complex, but a good Safeguards Provider can provide invaluable support. Use this to your advantage and stay vigilant in maintaining your program.

Summary

Maintaining an effective and compliant Safeguards Program is not a one-time task. It demands ongoing vigilance. Regular audits are an essential part of this equation. To maximize the effectiveness of your Safeguards Program, it's best practice to conduct full audits at least annually. Additionally, any significant changes in your business operations should trigger an audit to ensure compliance and security. Regular audits offer more than just compliance; they set your dealership on a path toward long-term security.

How Mosaic Can Help:

If you're interested in learning how Mosaic can assist your business in conducting Safeguards Program or deal jacket audits, contact us today!

Get Help