Safeguards Enforcement is Coming:

WHAT DEALERS SHOULD KNOW

MOSAIC
CYBER SECURITY

FTC Enforcement Plans

The afternoon sun was shining into a crowded room at the Wynn Las Vegas. We were three days into the National Independent Automotive Dealers Association (NIADA) conference, and this was the talk many of us had been waiting for. A lawyer from the Federal Trade Commission (FTC) was at the podium, carefully answering questions about the Safeguards Rule. Sitting next to him was a former FTC executive, translating the legal jargon into plain English.

Someone finally asked, "The Rule is live, but where are the perp walks? Will there be any Safeguards enforcement?" The lawyer responded, "Abso-freakin'-lutely!"

The FTC is planning a "sweep" of enforcement actions in the coming months.

The FTC is planning a "sweep" of enforcement actions in the coming months. A "sweep" is a coordinated enforcement that hits dozens of dealers at once, typically starting with larger groups. We've seen "sweeps" before with regulations like the Do Not Call Rule, Credit Repair, and various Advertising Rules. If history tells us anything, dealers shouldn't take this action lightly.

Even if a dealership isn't checked during the first sweep, that doesn't mean it's off the hook. If a dealership has a data breach, it will likely attract attention from the FTC and the plaintiff's lawyers. That's why it's so important for dealerships to fully implement the Safeguards Rule. Doing so will help prevent data breaches and the scrutiny that comes with them.

Who's at Risk?

Another audience member asked, "Who's on the blame line," if a dealership doesn't follow the Safeguards Rule properly? The FTC attorney confirmed that both the Qualified Individual (QI) and the Dealer Principal will be held accountable. As such, don't be surprised if your QI asks for a raise.

The first step to following the rules is understanding what you're currently doing at your dealership to protect customer information and what else the Safeguards Rule requires. Doing some of the things the rule requires isn't enough. While perfection may not be attainable, a consistent, good-faith effort to comply fully is both expected and achievable. Make sure your QI has the tools and support they need to ensure your dealership is following the rules and has an effective Safeguards program.

Are You Compliant?

The Rule is live and enforcement is on its way. The next step is to revisit your dealership's compliance program and double-check your Safeguards. To help, we've provided a comprehensive list of what's required by the FTC Safeguards Rule on the next page. If you answer "No" to anything on the checklist, Mosaic can help. Fill out our Safeguards Status Questionnaire and we'll provide a cost estimate to solve your compliance gaps.

Securing Your Dealership's Future

The FTC's planned enforcement of the Safeguards Rule is coming. It is incumbent upon dealerships to demonstrate a sincere effort toward achieving complete compliance. Remember, the goal of the Rule is to protect your dealership from a data breach. Investing in compliance is investing in your dealership's own well-being so you can keep selling cars. Mosaic offers dealerships complete and a la carte Safeguards compliance. Don't let your dealership be swept up in the wave of enforcement – take proactive steps toward compliance today.

Confirm What You Need

Safeguards Requirements Checklist

This checklist is intended to help you quickly gauge which Safeguards you have, and which you might need. **To get a quote please visit mosaiccs.com/quote.**

Do you run periodic Risk Assessments?
Risk Assessments should evaluate physical, administrative and technical security across the dealership.

Yes ☐ No ☐

Have you reviewed your service providers?
Review your service providers to ensure they acceptably protect the customer data you share with them.

Yes ☐ No ☐

Have you taken inventory of assets on your network?
Dealerships must take stock of all the devices on their network and understand the risk they pose.

Yes ☐ No ☐

Do you have Endpoint Detection and Response (EDR)?
EDR continuously monitors your devices 24/7 and stops cyber threats as they happen. While EDR is the only way to stop threats, this requirement may also be satisfied by a Pen Test and vulnerability scans.

Yes ☐ No ☐

Do you have multifactor authentication (MFA) and encryption?
Access to customer information must be gated with MFA and the data encrypted in transit and at rest.

Yes ☐ No ☐

Do you conduct simulated phishing?
While not a a requirement of the rule, most cyber breaches stem from a phishing attack. Do you train employees by sending fake phishing emails and provide training when they click what they shouldn't?

Yes ☐ No ☐

Do all employees take annual Security Awareness Training?
Training should address cyber and information security, and the consequences of a data breach.

Yes ☐ No ☐

Do you have a written Information Security Program (WISP)?
Your WISP details all the Safeguards have implemented at your store(s) and must include the following:

- Secure Development Practices
- Safe Data Disposal Policy
- Change Management Procedures
- Incident Response Plan

Yes ☐ No ☐

Do you produce an annual report on security?
Provide executive stakeholders with an annual "state of the union" report detailing the dealership's overall risks, safeguards, security events and remediation plans.

Yes ☐ No ☐

Do you perform audits of your Physical Safeguards?
Physical Safeguards includes keeping unauthorized persons away from non-public information that may be stored on your premises.

Yes ☐ No ☐