AUTOMOTIVE DEALERSHIPS AND THE FTC SAFEGUARDS RULE DEADLINE: IS YOUR INFORMATION SECURITY PROGRAM COMPLIANT?

How can automotive dealerships ensure they meet the new compliance requirements outlined by the updated Federal Trade Commission (FTC) Safeguards Rule by the December 8, 2022, deadline?

The Federal Trade Commission (FTC) announced several updates to the Safeguards Rule this past October with the intent of combatting cyber-attacks and safeguarding consumer information. Citing the widespread data breaches impacting consumers, the FTC updates aim to better protect consumers from breaches and cyberattacks that lead to identity theft and financial loss.

What must an automotive dealership's information security program include?

The nine required elements of an information security program are outlined in Section 314.4 of the Safeguards Rules:

1. Designate a "qualified individual" to implement and supervise your company's information security program.
2. Conduct a risk assessment to determine foreseeable risks and threats.
3. Design and implement safeguards to control identified risks from risk assessments.
4. Regularly monitor and test the effectiveness of safeguards.
5. Train staff by providing security awareness training and regular refreshers.
6. Monitor service providers with the appropriate safeguards (third-party risk management).
7. Keep information security programs current.
8. Create a written incident response plan that meets specific Safeguards Rule requirements.
9. Require the "qualified individual" to report to the Board of Directors or governing body.

Are any other institutions or businesses impacted by the FTC Safeguards Rule?

While the focus of this piece is on automotive dealerships, the updated FTC Safeguards Rule also applies to non-banking financial institutions, such as mortgage brokers and payday lenders.

How can Schneider Downs help automotive dealerships with the updated FTC Safeguards Rule?

The myriad of information security program requirements under the updated FTC Safeguards Rule has put a huge burden on automotive dealers who do not have the internal resources to meet the outlined security information requirements.

The Schneider Downs cybersecurity team and automotive industry group work together to provide the industry knowledge and technical talent to help automotive dealers meet the FTC Safeguards Rule's December 9, 2022 deadline.

If you have any questions about your information security program or the FTC Safeguards Rule, please reach out to me directly at ckriebel@schneiderdowns.com.

About Schneider Downs Cybersecurity

The Schneider Downs cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our Digital Forensics and Incident Response teams are available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

Want to be in the know? Subscribe to our bi-weekly newsletter, Focus on Cybersecurity, at www.schneiderdowns.com/subscribe.

The complete listings, requirements and details are available to view at:
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4.