
Hutchins


Fajgenbaum

What Automotive Dealers Need to Know About the Federal Trade Commission's New Cybersecurity Requirements

By Sarah Hutchins and Phillip Fajgenbaum, *Parker Poe Adams & Bernstein*

Automotive dealers will soon fall under a stricter version of the Federal Trade Commission's rule on safeguarding customer information. While many auto dealers are familiar with the old version of what's commonly called the Safeguards Rule, the new version is broader in scope, both in terms of who it applies to and what it requires.

On October 27, 2021, the FTC issued its final regulations amending the Safeguards Rule, which was promulgated by the FTC in 2002 pursuant to the Gramm-Leach-Bliley Act. Much of the new version will go into effect 30 days after it is published in the Federal Register, which an FTC spokesperson said could happen in December. But auto dealers will have close to a year to meet what are likely to be the biggest compliance hurdles, including new requirements for risk assessments, testing, and training. Some of those requirements will be a heavy lift that dealer counsel should start planning for now.

Many dealers will need to update and revise their existing information security programs. In fact, entities previously not subject to the Safeguards Rule may want to consider whether they are now within its scope, as the definition of "financial institution" is expanded to include entities engaged in activities "incidental to financial activities." This expansion ropes in auto dealers who may not have previously been subject to the Safeguards Rule.

At a high level, the old Safeguards Rule required financial institutions to develop, implement, and maintain a written comprehensive information security program for the purpose of protecting sensitive customer information. In doing so, financial institutions had to, among other things: (a) identify reasonably foreseeable internal and external risks, (b) design and implement a program to control the identified risks, (c) regularly test and monitor the program, (d) evaluate and adjust the program, and (e) designate an employee or employees to coordinate the program.

Given the lack of specificity in the old Safeguards Rule, dealers potentially had more flexibility in managing their information security. However, the new version now eliminates some of this elasticity by elaborating on many of the elements and adding more specific requirements. Among other things, the new rule makes the following changes:

- **Qualified Individual** – Financial institutions will be required to designate a single "qualified individual" responsible for overseeing, implementing, and enforcing their security program. The qualified individual will also be required to submit a written report, at least annually, to the financial institutions' board of directors, governing body, or, if neither exists, the senior officer responsible for the information security program.
- **Risk Assessment** – Risk assessments must now (a) be in writing, (b) detail the specific criteria that was considered in performing the assessment, (c) address how the risks identified will be addressed and/or mitigated, and (d) periodically be re-assessed to determine if safeguards should be modified or added.
- **Safeguards** – Safeguards must now address, among other things, access controls (both physical and electronic), secure development practices, data inventory, disposal procedures, monitoring, encryption, authentication, and change of management.
- **Testing/Monitoring** – Under the old Safeguards Rule, financial institutions had to simply "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures." The new rule goes further to require that such testing and monitoring include, in the case of information systems, either (a) continuous monitoring or (b) annual penetration testing and vulnerability assessments at least every six months.
- **Training** – Financial institutions must now add measures to ensure that personnel are effectively trained. In other words, dealers will now need to constantly update and revise their training. With respect to all employees, financial institutions must provide security training that is "updated as necessary to reflect the risks identified by the risk assessment." On the other hand, additional obligations are imposed with respect to "qualified information security personnel." Under the new rule, financial institutions must employ, in addition to the single "qualified individual," qualified information security personnel to manage the information security program. These specialized employees (or contractors) must be provided security updates as well as "training sufficient to address relevant security risks." Financial institutions must verify that these specialized employees are taking independent "steps to maintain current knowledge of changing information security threats and countermeasures."
- **Service Providers** – Financial institutions will now be required to monitor their service providers on an ongoing basis to ensure adequate safeguards.
- **Response Plan** – Financial institutions will need to establish a written incident response plan addressing seven specific areas. At

a high level, the response plan must address internal procedures, roles and responsibilities, information sharing, remediation, and documentation.

- **Exceptions** – Financial institutions with fewer than 5,000 consumers will not be required to comply with several of the new rule's requirements, including the sections focused on written risk assessments, continuous monitoring/testing, response plans, and periodic reports to boards or governing bodies.

There are more requirements beyond what we have touched on above, so dealer counsel would be wise to review the new Safeguards Rule in its entirety. This is an area where partnering with experienced cybersecurity and data privacy counsel can be valuable.

Undoubtedly, coming into compliance will prove costly for dealers and other financial institutions that have not regularly updated their training, safeguards, and response plans. To avoid the additional costs of noncompliance, dealer counsel should take action now to proactively update and revise internal policies, procedures, and safeguards – and document their dealership's efforts to do so. ■

Sarah Hutchins and Phillip Fajgenbaum are attorneys at Parker Poe in Charlotte, North Carolina. They can be reached at sarahhutchins@parkerpoe.com and phillipfajgenbaum@parkerpoe.com.

NADC Welcomes New Members

Fellow Members:

David Noll
McNees Wallace & Nurick
Harrisburg, Pennsylvania

Hilary Holmes Rheaume
Bernstein, Shur, Sawyer & Nelson, P.A.
Manchester, New Hampshire

Associate Member:

ComplyAuto
Hao Nguyen
Riverside, California