With new data security rules, dealers could face extra costs, need vendor cooperation

The cost of complying with the new regulations ultimately depends on how well dealers have been adhering to requirements under the original Safeguards Rule that took effect in 2003.

December 06, 2021 12:00 AM

AUDREY LAFOREST

WASHINGTON — Compliance with recent changes to the federal Safeguards Rule likely will mean extra upfront costs and operating expenses for U.S. auto dealerships, IT consultants and compliance experts say.

The cost of complying with the new regulations ultimately depends on how well dealers have been adhering to requirements under the original rule that took effect in 2003 and whether they've prioritized cybersecurity best practices at their stores, the experts told *Automotive News* last month.

Still, despite the potential cost burden, dealers must begin taking necessary steps to comply, including putting pressure on their technology vendors to ensure they can meet the new data security requirements.

"It's pretty substantial, and I think a lot of people are underestimating just how impactful this is going to be for dealers," said Chris Cleveland, compliance director for Galpin Motors in California.

In October, the Federal Trade Commission issued its long-debated final amendments to the Safeguards Rule. The amended rule beefs up the requirements financial institutions, including auto dealers, must implement as part of their information security programs to protect sensitive consumer data.

Dealers — and their service providers that access any customer data — have one year from the rule's publication in the Federal Register to comply with most of the new requirements, such as designating a "qualified individual" to manage their information security programs and preparing written risk assessments and incident response plans.

FINANCE & INSURANCE: WHAT'S NEXT?

Other requirements that largely mirror the existing rule take effect 30 days after publication. As of press time, the amended rule had not yet been published in the register.

SAFEGUARDS RULE REQUIREMENTS

Under the amended Safeguards Rule, which is mandated by Congress under the Gramm-Leach-Bliley Act, dealers will be expected to:

- Appoint a “qualified individual” to oversee, implement and enforce the information security program and submit an annual written report to the board of directors or governing body.
- Prepare a written risk assessment that can be used to evaluate and identify security risks periodically.
- Encrypt all customer information, both at rest and in transit over external networks.*
- Require multifactor authentication “whenever any individual — employee, customer or otherwise — accesses an information system.”*
- Implement policies and procedures for monitoring and logging the activity of authorized users and detecting unauthorized access to, use of or tampering with customer data by those users.
- Perform annual penetration tests and biannual vulnerability assessments.
- Ensure personnel are able to enact the information security program by providing security awareness training and other training programs that are updated as necessary.
- Oversee and monitor service providers, and assess those providers after onboarding.
- Adopt a written incident response plan.

‘New ballgame'

The National Automobile Dealers Association said it is advising its franchised dealer members to make sure they're fully complying with the current requirements and that they also contact their technology vendors as soon as possible to ensure they can meet new obligations under the amended rule.

"We'll see how the next year progresses, but it is going to be complicated," said Brad Miller, NADA's director of legal and regulatory affairs. "It's going to be — unfortunately, we fear — expensive. And it's going to require a lot of

attention from dealers, and they're going to have to do a lot of things that may be new or well beyond their current procedures."

NADA leaders raised multiple concerns about proposed changes to the rule in public comments to the FTC in 2019 and 2020, and also submitted a cost analysis that indicated U.S. dealerships could face billions of dollars in additional compliance costs if they were adopted. In total, the association estimated U.S. franchised dealerships would need to shell out $2.2 billion in initial startup costs, followed by $2.1 billion in annual costs.

NADA said it has not updated the cost analysis for the final rule but doesn't expect the estimates to be materially different.

"In terms of having the expertise and investment that this is going to require," Miller said, "it's going to be a whole new ballgame for most dealers."

Tony Martinez, vice president of cybersecurity solutions at MGT Consulting, said while it's difficult to pinpoint the exact cost for dealers, they need to start making cybersecurity a core competency of their coporate operations.

"This is going to be an ongoing operating expense. This isn't a capital expense that's 'set it and forget it,' " he said. "You're never going to be done with security."

Vendor pressure

Larger dealership groups are likely better positioned to comply with the new requirements — and may already be doing so. But for smaller retailers, especially one-rooftop dealers, "this is really going to be the game-changer for them because a lot of this stuff they're probably not doing today," said Cleveland, who also is CEO of ComplyAuto, a company that uses cloud-based software to help dealerships navigate data privacy regulations.

Of the rule's changes, one of the most significant for dealers is the requirement to implement multifactor authentication for any system containing nonpublic personal information.

"Most dealerships just rely on vendors to store their information, and so it's going to be a lot of pressure putting on these vendors to implement [multifactor authentication] on the dealer's behalf because, ultimately, it's going to be the dealer's responsibility," Cleveland said.

Dealership management system providers are considered service providers under the Safeguards Rule, and dealers must require them by contract to protect consumer information, according to the FTC.

"The previous version of the rule and this version continue to have a requirement to oversee these service providers you have regarding safeguarding and making sure that they have a compliant safeguards program," said Dailey Wilson, an associate at the Hudson Cook law firm.

DMS giants CDK Global and Reynolds and Reynolds both told *Automotive News* they were working with their customers to address the new requirements.

"Reynolds has long been a proponent and leader in improving data security in the automotive industry," Greg Uland, vice president of brand marketing, said in an emailed statement. "As new regulations go into effect, we continue to work with our dealer partners to help ensure they have the tools they need."

Uland said the company's Era-Ignite system provides multifactor authentication functionality and encrypts data across the dealership's network — two requirements under the amended rule.

CDK Global spokesman Tony Macrito said the company is "committed to providing compliant solutions for our customers on the timeline required under the rule" and is encouraging dealers to start taking steps toward compliance.

"Overall, I don't think any of this stuff is unreasonable," said Cleveland, citing data collected by dealerships such as Social Security numbers, credit reports and bank accounts. "We should be held to these kinds of standards. It's just common sense."

'Broad brush'

James Ganther, CEO of Mosaic Compliance Services, argues that for dealers the new requirements have the potential to be "extraordinarily onerous."

"In the dealership environment, I could argue that much of this is overkill," Ganther said. "It's such a broad brush. 'Financial institutions' is such a broad category, and I don't think anyone would say the level of data security for American Express is the same as the car dealership up the street."

Entities that maintain 5,000 or fewer consumer records are exempted from several of the new requirements, such as the written risk assessments. But NADA leaders and compliance experts say few, if any, dealers would likely be eligible.

Michael Alf, general manager at St. Charles Toyota in Illinois, said in addition to making sure his store's third-party vendors comply with the new rule, the biggest burden likely will be appointing a qualified individual to oversee the information security program.

"That's going to be one of the largest expenses besides the hardware and software," Alf said.

Dealers don't need to hire highly paid chief information security officers under the new requirements, but instead must select an individual with "some level of information security training and knowledge," said Randy Henrick, president of dealership compliance firm Randy Henrick & Associates.

"The exact qualifications will depend on the nature of the dealer's information system, and the volume and sensitivity of the customer information that the dealer possesses or processes," he said.

For groups with multiple rooftops and similar risk assessments, "there could be one person who assumes that role for each entity and does it for more than one entity in a group," Henrick said.

While dealers might not see a tangible return on investment, Brad Holton, CEO of dealership IT consulting firm Proton Technologies, said "if you don't do it, you will certainly see a significant, potential loss."

"If the dealer is actively engaged in hardening their network and focusing on cyber hygiene and cybersecurity," he said, "then this is not that big of a reach outside of what I would normally expect them to be doing anyway."

Despite any upfront and ongoing costs, Erik Nachbahr, president of dealership IT company Helion Technologies, said taking steps to prevent data breaches is worth the investment.

"You have one of these big attacks: What does that do to your reputation?" Nachbahr said. "Protecting that, I think, is another key piece to all of this."