NADC
National Association of Dealer Counsel®

DEFENDER

The National Association of Dealer Counsel Newsletter Volume XVIII, Number 9
OCT 2024

In this Issue:

2025 NADC Annual Member Conference

May 4-6, 2025

The Ritz-Carlton Golf Resort, Naples
Naples, FL

SAVE THE DATE

Contact Us:

NADC
1800 M Street, NW
Suite 400 South
Washington, DC 20036
Phone: 202-293-1454
Fax: 202-530-0659
info@dealercounsel.com
www.dealercounsel.com



Sprinkle *Hutchins* *Snowden*

What Automotive Dealers Should Know About State and Federal Cybersecurity and Data Privacy Actions

By Todd Sprinkle, Sarah Hutchins, and Hunter Snowden, *Parker Poe*

Cybersecurity breaches this year have hit most major industries, from health care to financial services to education. Automotive dealers are also firmly on that list.

When a major software provider for dealers experienced a significant cybersecurity breach over the summer, it highlighted how disruptive these incidents could be. Dealers that relied on the software for vehicle sales, financing, and customer relationship management were impacted by an outage that reportedly adversely affected business.

It also highlighted how few industries are safe from such cyberattacks, particularly as vehicles become more connected to drivers and their personal data.

For dealers, incidents like these are good reminders about the importance of maintaining a vigilant cybersecurity posture, including at the vendor level, and implementing robust procedures to report cyber incidents in a timely manner. Dealers must also be aware of how a patchwork of data privacy laws impact their disclosure and retention obligations regarding collection of personal data.

Agencies like the Federal Trade Commission and others including state attorneys general have automotive dealers' cyber-readiness on their radar, as well.

Here's a look at what automotive dealers need to know about data collection and state and federal action.

State, Federal Regulators Zero in on Auto Dealer Privacy Practices

State regulators are investigating automotive dealer privacy practices and compliance is firmly placed on the auto dealers' shoulders. With penalties applied on a per violation basis, these investigations are part of the rapidly

growing risk posed to dealers by a patchwork of data privacy laws.

Some states are asking even more of dealers through dealer-specific laws like providing privacy notices prior to sale or lease of a new car equipped with an in-vehicle camera (California) or deleting any personal data on a used car's computer system prior to repurchase or lease (New Jersey).

In Texas, the attorney general filed a complaint in August against an automotive manufacturer, alleging that it failed to disclose the telematics data it collected and subsequently sold to third parties, without the consumers' consent or knowledge. This action could serve as a roadmap for other state attorneys general, given the legal basis of the action stems from the Texas Unfair and Deceptive Trade Practices Act, of which there is an equivalent in every state along with Section 5 of the Federal Trade Commission Act.

The FTC is active in ensuring cybersecurity in the auto industry. As part of its focus on the dangers of new technology, the agency posted a technology blog in May about connected cars that could be collecting sensitive data such as biometric information or location.

The FTC attempts to enforce baseline standards for information collected through the financing process through the Gramm-Leach-Bliley Act's Safeguard Rule. This rule requires financial institutions to develop, implement, and maintain a written comprehensive information security program for the purpose of protecting sensitive customer information. These requirements were enhanced through the FTC's update to the Safeguard's Rule in 2023.

The rule's expansion ropes in auto dealers who may not have previously been subject to the Safeguards Rule. Partnering with outside counsel can be valuable to determine compliance and update training, safeguards, and response plans.

SEC Zeroes in on Data Security and Reporting

Publicly traded auto dealers should also be aware of recent U.S. Securities and Exchange Commission action related to cybersecurity incidents. Under a final rule released last year, public companies and certain foreign private companies have to take additional steps after cybersecurity breaches, including deciding whether an incident meets the materiality threshold that requires disclosure pursuant to SEC rules. Public companies also have to enhance their periodic disclosures related to their cybersecurity risks, management, and strategy, per the final rule.

For automotive dealers, developing a strong incident response plan before an actual incident is critical to ensuring compliance with reporting obligations. Incident response plans should require proper oversight and proactive communication with legal and information technology functions to fulfill corporate governance obligations.

Final Takeaway

The use of technology in customer engagement and the prevalence of increasingly connected cars means automotive dealers need to be aware of vulnerabilities around cybersecurity breaches. Federal data privacy laws have certain requirements for the safeguarding of sensitive customer information and agencies like the FTC have been closely watching the automotive industry. Dealers should be vigilantly preparing for breaches by developing training around their incident response policies and plans.

Todd Sprinkle is a partner in Parker Poe's Atlanta office. His practice includes all aspects of civil litigation, both state and federal, at the trial and appellate levels. Todd focuses on business litigation, financial services litigation, real property dispute resolution, trade secrets, and alternative dispute resolution. He sits on the NADC board of directors.

Sarah Hutchins is a partner in Parker Poe's Charlotte office, serving as the firm's Cybersecurity & Data Privacy Team leader. She is certified as a legal specialist in privacy and information security law by the North Carolina State Bar. Sarah helps clients navigate business litigation, government investigations, and data privacy and cybersecurity

Hunter Snowden is an associate in Parker Poe's Charlotte office. He helps businesses navigate the complex and evolving legal landscape of data privacy, cybersecurity, and technology transactions as well as the routine transactional needs of clients. Hunter has experience in various industries including technology, finance, manufacturing, automotive, retail, real estate, and government relations.