CDK Breach Update – Next Steps for Dealers

By
Tom Vangel, Esq.
James Radke, Esq.
Lindsey McComber, Esq.
Murtha Cullina LLP

Last month's CDK data breach wreaked havoc on the automotive community and caused major disruptions to the business operations of approximately 15,000 dealerships across the U.S. and Canada. The attack paralyzed the operations of nearly all dealerships relying on the CDK software, and, as a result, these dealerships were forced to use manual processes, which slowed sale operations significantly during one of the busiest seasons in the industry.

Although the public has not been made aware of the full effect of the breach and what information was stolen, it has been reported that the breaches exposed the financial information, sensitive customer data, and driver's licenses for tens of thousands of dealership customers. In addition, during the outage, sales representatives at various dealerships struggled to close and finance deals, with the full financial impact of the attack still to be determined. Although CDK Global's CEO has told dealers that the company will compensate them in some way, it is unclear when or how much compensation dealers will receive.

As a result, many dealerships filed lawsuits against CDK that are still in the early stages of litigation. In Complaints that were filed in the U.S. District Courts for the Northern District of Illinois and the Southern District of Florida, the plaintiff dealers allege that CDK negligently failed to protect consumer information. They claim that this negligence exposed consumer personal information and brought sales, financing, and payroll operations to a halt and, therefore, are seeking damages arising from the loss of business.

Many dealers are asking what changes can be made to avoid or mitigate these risks in the future. While it appears impossible to eliminate the risk of a data breach in today's digital world, there are certain immediate steps that dealers can take to mitigate their losses and liabilities from the CDK breach and protect their businesses in the future. These include ensuring that the records of sales completed during the outage are properly accounted for, informing themselves about their reporting obligations to state and federal regulators, starting the claims process for any applicable cyber insurance policy, and reviewing vendor contracts.

Although the CDK software is now restored, it may still take weeks or months to get all the data restored and for operations to return to normal. Dealers must ensure that their accounting departments assemble and properly account for business transacted during the outage. Further, dealers must stay up to date on their data breach notification obligations. CDK reached an agreement with the Federal Trade Commission to permit CDK to file a single, consolidated breach notification on behalf of all affected dealers, which will satisfy any obligation on the part of individual dealers to file a breach notification with the FTC.

However, Massachusetts law requires any business that experiences a breach of the personal information of any Massachusetts resident to notify the affected customers and the Attorney General as soon as practicable following the discovery. Dealers will need to work with their counsel to prepare and submit a breach notice if and when they learn that the personal information of their Massachusetts customers has been unlawfully accessed.

Dealerships with cyber insurance in place should review their claims reporting obligations under their policies. It is recommended that dealers notify their insurance providers as soon as possible and that they quantify and maintain proper documentation of the financial impact of the business interruption. Dealers also should review carefully their vendor contracts to determine their contractual obligations regarding data security and breach notification. These contracts may also address indemnification issues, liability limitations, and whether vendors are required to produce information to the dealer about actual or suspected breaches.

The CDK incident has highlighted the vulnerabilities dealers face when working with third parties for services. At a minimum, dealers should assess their current dependency on third party systems, make any necessary changes, and continue to invest in IT audits and cybersecurity programs. Additionally, it would be beneficial for dealers to seek advice from qualified experts to devise a long-term plan for data security and to establish their own breach protocols. This would require dealers to perform their own due diligence with retained experts and legal counsel.

The CDK cyber-attack is undoubtedly one of the worst attacks affecting dealers in recent memory. However, it serves as an important reminder that dealers should take a careful look at the systems that they are using and determine whether they are adequately protected in the case of a future cyber-attack. Dealers should perform their own due diligence and work with experts and their attorneys to come up with long-term data security and continuity plans to ensure that their businesses are protected.

Tom Vangel, Jamie Radke, and Lindsey McComber, with the law firm of Murtha Cullina LLP in Boston, specialize in automotive law and can be reached at (617) 457-4072.