COMPLYAUTO

CDK Ransomware Incident (June 2024)
Dealer Response Checklist

Below are some steps that dealers using or formerly using CDK products should consider if they believe CDK still has their data.

☐	1. Ensure the dealer's full compliance with the revised FTC Safeguards Rule.
☐	2. Consider achieving compliance with a nationally recognized cybersecurity standard, such as the Center for Internet Security (CIS) Controls, as this may provide safe harbor from data breach liability in some states.
☐	3. Consult with counsel regarding obligations and strategy. Added benefit is that discussions with counsel are likely protected under the attorney-client privilege.
☐	4. Implement basic cybersecurity protocols, such as implementing endpoint detection and response (EDR), multi-factor authentication (MFA), phishing simulations, penetration testing, vulnerability scanning, network segmentation, and performing offline backups.
☐	5. Make a written request to CDK for details about the details and scope of the incident.
☐	6. Consider notifying relevant insurance carriers of potential claims (e.g., cyber insurance, general liability, business interruption).
☐	7. Review contract with CDK for CDK's obligations pertaining to data breach, indemnification, etc.
☐	8. Have a PR strategy for both external and internal communications.
☐	9. Consider what, if any, remediation services the dealership may want to offer. Consider if insurance coverage will cover these costs.
☐	10. Determine how payroll will be processed if financial statements and sales data are not available by payroll date.
☐	11. Consider reaching out to DMV and state agencies. Your state dealer association may be able to help.
☐	12. Consider whether the incident poses issues with other vendors (e.g., payments, DMS connections) and discuss with vendors accordingly.
☐	13. Evaluate the obligations related to data breach notifications under Federal and State laws if it is ultimately confirmed that personal data was affected. Weigh the advantages and disadvantages of reporting the incident now, even before fully understanding its scope, against waiting until it is confirmed whether or not personal data was involved.
☐	14. Secure systems from bad actors looking to take advantage of the situation and potential future attacks against the dealership.
☐	15. Establish a business continuity plan for future incidents.
☐	16. Keep records of the steps the dealership has taken to minimize risk, monitor vendors, and investigate incidents.