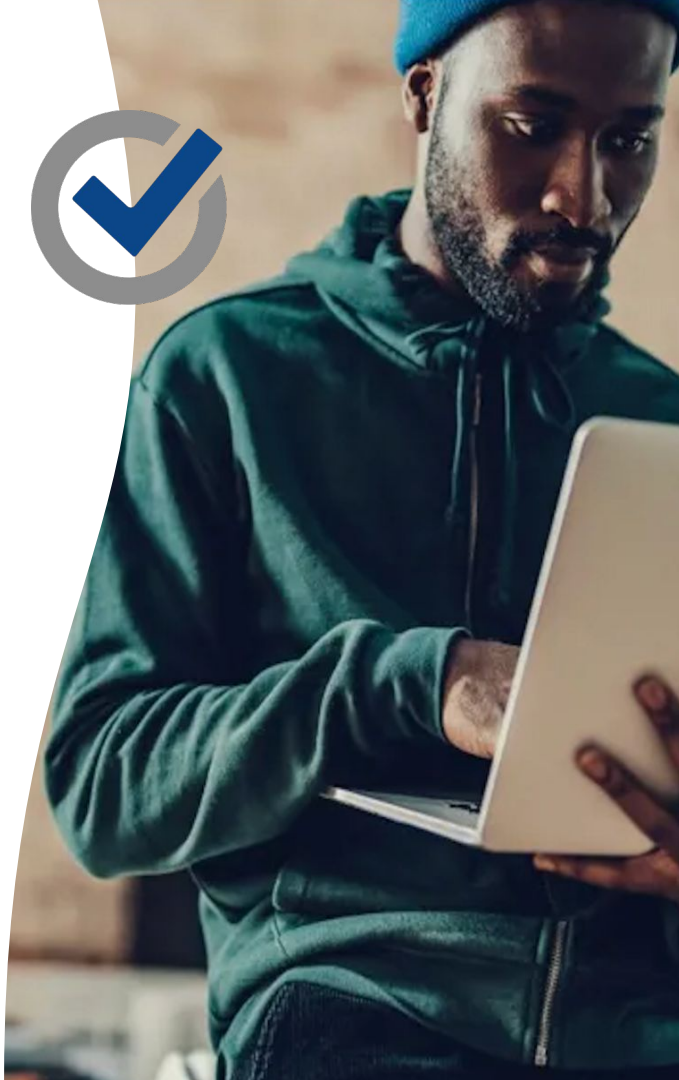
COMPLYAUTO

CDK Cyber Incident

Update and Guidance

June 27, 2024



Legal Disclaimer and Notice

This presentation is intended to be used as a compliance aid. Reasonable efforts have been made to ensure the accuracy and completeness of the following subject matter. No express or implied warranty is provided respecting the information contained in this presentation. **The following material is not legal advice and should not be construed as (nor used as a substitute for) legal advice.** If legal advice is required, the services of a competent professional should be sought. Each dealer must rely on its own expertise and knowledge of law when using the material provided.

This webinar, and your participation in the webinar, may be monitored, recorded, and shared. This presentation is the property of ComplyAuto Privacy LLC.

The Presenters

Christopher Cleveland

Co-Founder & CEO

10+ years
as Compliance Director
at a large dealership group

Brad Miller

Chief Compliance/
Regulatory Officer
Head of Legal

16+ years
Chief Regulatory Counsel
National Automobile Dealers
Association

COMPLYAUTO

Agenda

- Brief Update on CDK Incident
- What Should Dealers Do Now?
  - Practical, Legal, and Regulatory Considerations
  - Notice Considerations
  - Technical Mitigation Steps
  - Limiting Potential Liability
- What is ComplyAuto Doing to Help All Dealers?

COMPLYAUTO

Latest on CDK Incident

- CDK has not officially confirmed anything other than it was a "ransom event." CDK has announced that it beginning to restore DMS functionality, but that it is unlikely to be resolved before 6/30/24
- Several class action lawsuits filed (including claims of unreasonable delay in informing consumers)
- Several public reports - Blacksuit ransomware (formerly known as Royal) - Eastern European crime syndicate
  - CISA description is malware, customer data download, and encryption of system
  - CISA remediation tips for Royal - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
    ComplyAuto assists dealers in taking most/all of these steps
- OEM reaction has varied
  - Some providing tools and workarounds
  - Addressing warranty and other reporting tools
  - Reminding dealers that they should take steps to protect themselves
  - Obviously, reach out, if you have not already done so
  - Some OEMs have indicated they will be exercising audit rights over CDK


CDK cyberattack will add to dealership regulatory stresses

The FTC Safeguards Rule requires dealerships and other financial institutions to notify the agency after it discovers a security breach involving the information of at least 500 customers.

MARK HOLLMER

RECOMMENDED FOR YOU

CDK Global shutdown forces dealers to pivot

A cyberattack is obviously never a good thing. But the June 19 attack that

management system provider with thousands of customers across the co

clients.

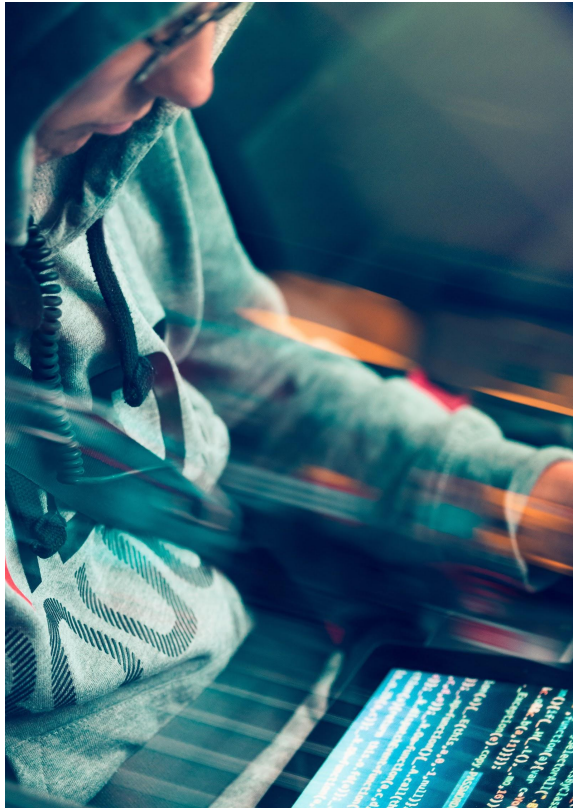
That's because dealerships are facing heightened federal regulations regarding data privacy that have already added cost and agitation to the equation. They also may face more public scrutiny even though this attack didn't affect them directly.

Latest on CDK Incident

- Dealer Reaction
  - Operational challenges continue
  - Workarounds in place - but end of month/end of quarter looming
  - ComplyAuto has seen marked spike in pen test and other related activity among customers

- Reports of outage at another large dealer group - no indication of connection between incidents. But of note (class action lawsuit) allegation - Scattered/Spider/ALPHV

  "Scattered Spider is suspected of working with a group called AlphV/BlackCat, using a voice-phishing technique to trick IT support or call center workers into bypassing multifactor authentication."[1]

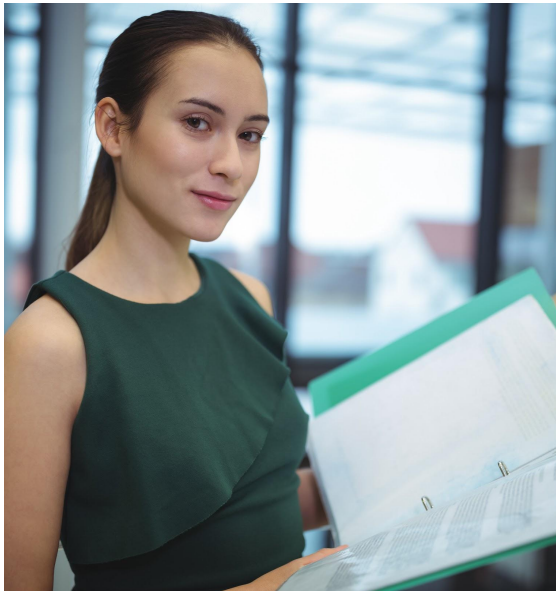


[1] https://www.cisa.gov/news-events/alerts/2023/11/16/fbi-and-cisa-release-advisory-scattered-spider-group

COMPLYAUTO

What should dealers do now?

Practical, Legal, and Regulatory Considerations



Make a written request to CDK

- ➔ Document a formal request for details about
  - The incident generally
  - Whether any dealer data was affected
  - Whether a specific dealer's data was affected and if so
    - How many records?
    - What states were they residents of?
- ➔ May want to consult / engage counsel

NOTE: Many states have a "vendor cooperation" requirement that you could cite

Ex: Virginia

Third-Party Data Notification. "*An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the PI was accessed and acquired by an unauthorized person or the Entity reasonably believes the PI was accessed and acquired by an unauthorized person.*"

What should dealers do now?

Practical, Legal, and Regulatory Considerations

- CDK may or may not be able to tell you anything at this time (and may be for a good reason)

  But that is, in some ways, less important for you than the fact that you asked
- REMEMBER
  - This includes all CDK products - not just the DMS
  - May or may not be affected, but still need to ask
- If, at some point, they respond "no, not affected" to your inquiry - that is likely not enough
- Burden of proof is on *you* to show that it could not have affected your customer data

COMPLYAUTO

What should dealers do now?

Practical, Legal, and Regulatory Considerations

- Notify Relevant Insurance Carriers? - put on notice of a potential claim
  - Cyber Insurance - if you have, determine scope of coverage
    - Does it cover customer breach notice costs?

      Will affect your choice re: State breach law consumer notice
    - Systems recovery costs?
  - Business interruption? - may be in Garage or CGL policy
- Consider whether you will offer appropriate remediation services (e.g., credit monitoring)
  - A number of state breach notification laws may require this to be offered w/ notice
  - Does your insurance cover these costs? - can be significant
- Look at your contract with CDK
  - Did they sign the required GLBA Safeguards Rule agreement?
  - What does it say about downtime and data breach liability?

What should dealers do now?

Practical, Legal, and Regulatory Considerations

- Have a PR strategy - Develop a clear communication approach
  - Be prepared to address customer concerns and potential complaints
  - Press inquiries
  - Centralize consumer responses - ensure your staff is not giving contradictory information
  - Any assurances for your customers after the dust settles?
- Outreach to DMV/state agencies? (work with your ATAEs/State Associations)
- Your vendors? (payment and other issues)
- Establish a business continuity plan?
  - To prepare for the next time
  - A number of our customers have reported significantly reduced impacts
  - Preparation - combination of policies/technology/practice (table top)
  - ComplyAuto will be releasing a BCP policy builder in the future

What should dealers do now?

- Continue to investigate as possible, the impact on your consumer data - and get ready to notify
- Safeguards Rule
  - NEW RULE! - Must notify the FTC “as soon as possible” and no later than 30 days after “discovery” of a “notification event”
  - Must report to the FTC by filing a report on the FTC website
  - Will be made available in a publicly available database
  - Discussed in greater detail below - but check with your lawyer before deciding!
- State Data Breach Notification Law (all 50 states)
  - Sample state notification letter - in ComplyAuto ISP
- ComplyAuto Breach Notification and Reporting Analysis Tool
  - Determine if you have access to consumer databases to even send consumer notice
  - May want to explore the tool just so you have a general understanding of what you may need to do

Notify the FTC Now or Wait?

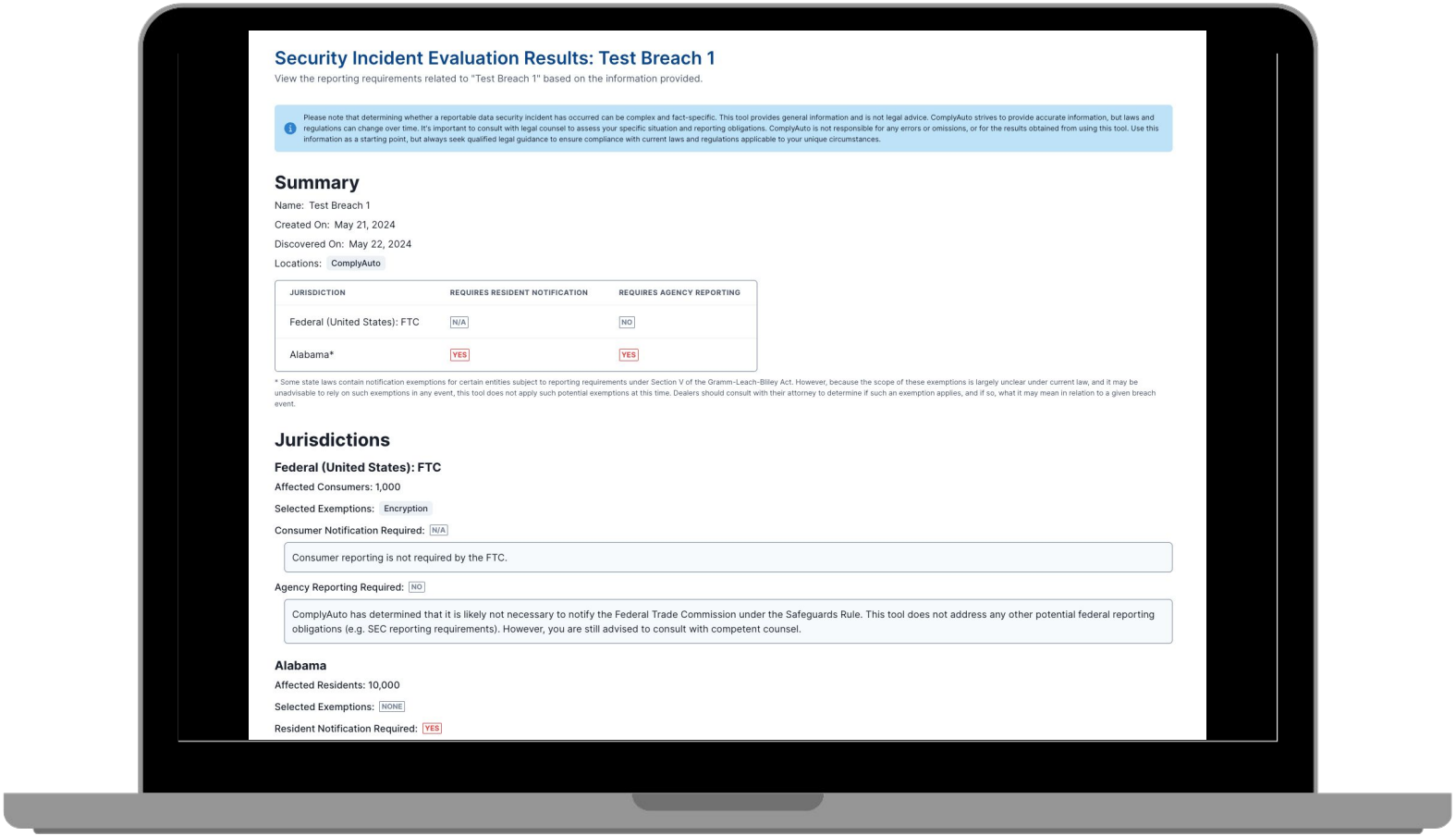
PROS

- Ensures you don't miss any FTC deadline
- Meets your Safeguards Rule reporting obligation
- Allows for reporting of what you know today (which is basically public information)
- FTC public database does not yet appear to be operational
- No duty to "update"
- Could diminish risk of a claim that you failed to timely notify consumers.

CONS

- Will be among the first to publicly report
- Will be available in a publicly available database (same as several states however)
- Will of course be muted as more dealers report
- Will be in YOUR name, not CDK
- Cannot file under state law, so does not meet all potential obligations
- Will be notifying the public that you are a CDK user
- Could trigger scrutiny from FTC and plaintiff attorneys

New Breach Notification and Reporting Evaluation Tool



Sample Breach Notification Template

Appendix A: Sample Data Breach Notification Letter

ComplyAuto, Date: *[Insert Date]*

NOTICE OF DATA BREACH

Dear *[Insert Name]*:

We are contacting you about a data breach that has occurred at ComplyAuto

What Happened?

[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].

What Information Was Involved?

This incident involved your *[describe the type of personal information that may have been exposed due to the breach].*

What We Are Doing

[Describe how you are responding to the data breach, including: what actions you've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services)].

What You Can Do

[Insert the following language if the information compromised poses a high risk of identity theft or social security numbers were compromised].

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts

in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

[Insert the following language if you choose to provide a copy of the FTC's identity theft guide].

We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Other Important Information

[Insert other important information here]

For More Information

Call *[telephone number]* or go to *[Internet website]. [State how additional information or updates will be shared/or where they will be posted].*

[Insert Closing]

[Your Name]

What should dealers do now?

Technical Mitigation Steps

- **Remediate Vulnerabilities:** Perform penetration testing, vulnerability scans, and regularly update and patch systems.
- **User Training:** Train employees to recognize and report phishing.

NOTE: ComplyAuto has CDK-specific phishing template available now

- **Authentication:** Enforce multi factor authentication (MFA) and use strong, unique passwords.
- **Network Security:** Segment networks, disable unused ports, and apply least privilege (PoLP).
- **Backups:** Maintain encrypted, offline backups and regularly test restoration.
- **Detection & Response:** Use endpoint detection and response (EDR) tools, monitor network traffic, and update antivirus software.
- **Additional Measures**: Disable command-line activities and add email banners for external emails. Use email security tools and automated spam/phishing filters.

What should dealers do now?

Limiting Potential Liability

- Dealer Liability? Complicated question, but need to prepare:
- Protect your internal systems from further problems (see mitigation steps above)
  - Work with all your vendors
  - Remember that in some states, your liability for a breach is limited if you meet certain cybersecurity standards - ComplyAuto can help
- Notify and keep informed
  - Agencies and consumers
- Investigate what you can investigate internally and with all potentially affected vendors
  - You want an answer to: "What did you do to ensure that this did not affect other systems or data?"
- Ensure compliance with state privacy laws (not just the data breach laws)
  - 19 states now have laws - often have data security components and data breach liability
- Make a record - Of all the steps you have taken

COMPLYAUTO

What should dealers do now?

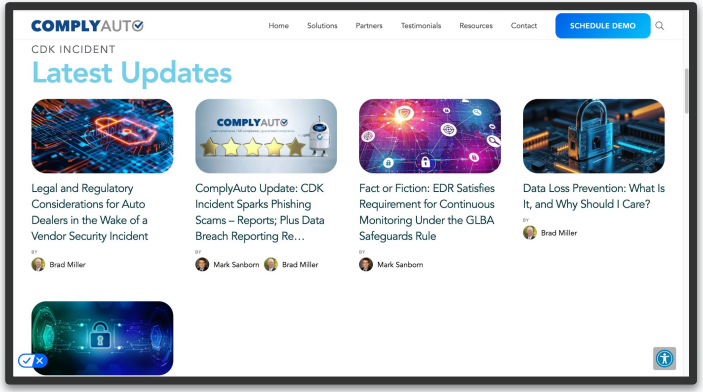
Limiting Potential Liability

- ➔ Ensure *complete* Safeguards Compliance
  - First step in any claim:"Show me your Safeguards materials"
  - Update as required in the wake of an "incident"
    - Vendor review
    - Information Security Program Update
    - Board report - NOTE*
  - Vendor "audits"
  - ComplyAuto has most complete suite of tools available to dealers.
- ➔ Review contracts and be prepared
  - Safeguards compliance
  - Breach notification obligations
  - Indemnification
  - Data Security representations

How is ComplyAuto Here to Help?

- Full suite of remediation tools that we provide
  - Aligns with what CISA recommends
  - Our Breach Reporting Analysis Wizard
  - Sample Breach Notification Letters
  - Safeguards Rule Compliance Update tools
  - Vendor contracts
- We are stepping up to do more!

Therefore, we are making available to ALL dealers at no charge . . .



VISIT COMPLYAUTO'S
CDK INCIDENT RESOURCE CENTER
for up-to-date info and insightful articles about best practices, FAQs, and tips

www.complyauto.com
click Resources

90 days FREE

no billing information required

dealer+secure compliance suite

email security solutions + phishing simulations + FTC Safeguards Rule compliance

CORO

Email Protection Suite

- Phishing Protection
- Malware Scanning
- Domain & Impersonation Spoofing Detection
- Suspicious Attachment Filetype Blocklisting
- Domain Allow/Block Lists

COMPLYAUTO

Phishing Simulations

- Dealer-specific templates
- Easy-to-use Interface
- Testing & Training
- Fully Managed

FTC Safeguards Rule Compliance

- 50-state Data Breach Reporting Wizard
- Incident Response Plan Builder
- Guided Risk Assessments
- Employee Training
- Vendor Management
- Data Mapping

We’re here to help! Questions?

chris@complyauto.com

brad.miller@complyauto.com

10,000+ active dealers across all 50 states

40+ state dealer association endorsements

NADA AFFINITY PROVIDER

dealer+secure compliance suite