Testimony of Chris Anderson
CDK Global
Joint Transportation Committee Hearing re HB 3152
May 1, 2019

I am Chris Anderson, and at CDK I am the person most responsible for our Dealer Management System - or "DMS" - that is featured in this legislation.

The DMS is a productivity tool. After 15 years at CDK I can say without reservation that our goal has always been to help dealers transact business efficiently and profitably, and without having to think for a moment about computers, IT, data security, consumer privacy or hackers. Our DMS simplifies back office and administrative work so dealers can focus on their core business - selling and servicing cars and making their customers happy.

Every time a dealer has a new task, process requirement, or business partner, our job is to build it into the DMS to simplify the dealer's life. We also capture every transaction in the dealer's financial and business records so there is transparency when managers review sales and service teams, when accountants prepare tax filings and when bonuses are determined. Typically the DMS also houses employee records, including payroll, banking and tax information.

The DMS provider is a data processor, not a data controller. DMS rules about who gets to connect and who can access data are determined by laws or contracts - including federal and state consumer protection laws and contracts negotiated with dealers, manufacturers and hundreds of partners that provide data to dealers or utilize data provided by dealers. All that data flows through the DMS and the laws and contract requirements are implemented through software.

By mandating that unlicensed, unmonitored third parties can access, copy, distribute and even sell consumer and business data that they do not own and that dealers do not own, this bill would require CDK to violate contracts with auto manufacturers, banks, credit reporting agencies and many more partners that provide data to our DMS for very specific purposes, and that instruct us to limit access to that data so it only goes to parties that perform specific services that require the data.

This legislation permits <u>any</u> dealer business partner to be designated an integrator and get CDK services for free. Moreover, it prohibits CDK from shutting off a dealer's DMS service even if the dealer refuses to pay for the service - ever. How can CDK continue to employ high-wage team members, service dealers and other customers and improve our products if we are required to give away our valuable intellectual property and all associated services? Why would this Committee approve of dealerships taking our services for free, taking data that is owned by others, or forcing open otherwise very secure databases?

Please oppose this legislation. Thank you

Testimony of Mike Noser
CDK Global
Joint Transportation Committee Hearing re HB 3152
May 1, 2019

Good evening. I am Mike Noser, and I oversee CDK's Partner Program and security operations for the CDK DMS.

DMS partners, to support their business with dealers, put data into or take data out of the DMS. Our hundreds of partners include auto manufacturers, banks that provide financing, insurance and warranty companies, credit rating services, and specialty companies like Carfax and Cars.com.

Partner contracts require CDK to use state-of-the-art technology and rigorous processes to protect their data. Today CDK accomplishes this by requiring partners to retrieve or contribute data through customized certified interfaces that ensure each connection to the DMS transmits all the data needed but only the data that is needed. This principle - sharing the minimum amount of data to the minimum number of people necessary - is fundamental to good data management that both facilitates commerce and protects privacy and confidentiality.

Like all enterprise systems providers, CDK and the DMS industry have invested hundreds of millions of dollars to improve data security in the last several years. Some dealers and certainly all the unlicensed integrators may be frustrated by this, but our purpose is clear-- to protect data stored on the DMS—much of which is not owned by CDK or by the dealers licensing our DMS-- and in doing so to comply with federal and state law and our contracts.

I also oversee DMS security operations. CDK has invested in technology and a dedicated team that monitors for unauthorized intrusions and that implements security features like CAPTCHA - a product you may be familiar with because Ticketmaster, Google and others use it to stop automated robotic software from accessing their systems.

Today, on behalf of dealers, auto manufacturers, banks and the consumers they work with, CDK controls access to the DMS to protect the data in the DMS and maintain the integrity of the DMS system so that we can provide the best possible customer experience. The access controls and security protocols are required by laws and contracts, including our contracts with dealers.

CDK is undertaking a massive effort to comply with the European General Data Protection regulation and the California Consumer Privacy Act, and we expect that the FTC will also tighten data security rules that apply to the automobile industry. These are the trends of governments and all companies that manage data. But HB 3152 goes in the opposite direction.

I urge you to oppose HB 3152.

Testimony of Dean Crutchfield
CDK Global
Joint Transportation Committee Hearing re HB 3152
May 1, 2019

Committee Chairs and Members:

I am Dean Crutchfield, Executive Vice President and Chief Information Officer of CDK.

1. I manage the IT infrastructure for all of CDK. Chris Anderson spoke of how he manages the DMS; it's my job to ensure that he has the technology resources to operate a best-in-class service.

2. I manage the global security organization. It's my job to make sure that hackers do not access the DMS or other computer systems that CDK manages, because if they get in then the system can be corrupted and terabytes of data – including consumer information and data that other companies and dealers themselves own and entrust to us - can be corrupted or stolen.

3. I supervise the incident investigation team. In an average month we investigate between ten and twenty information security incidents, ranging from minor to substantial, and involving our own intellectual property, hostile intruders to our system, or dealers that have been compromised.

In a recent survey, an alarming 85-percent of IT-related auto dealer employees reported that their dealership suffered a cybersecurity incident in the last two years. Nevertheless, 66 percent of dealerships have not conducted a formal risk assessment to help anticipate cybersecurity risks; 65 percent do not regularly test their IT security systems and processes; and 63 percent do not have formal response processes in place that can be activated after breaches in their network. The automobile industry needs more security conscious technology providers because managing sensitive data is a complex undertaking.

There are good reasons why dealerships outsource their Dealer Management System, and why manufacturers, banks, credit reporting agencies and other partners prefer that their data be professionally managed by companies whose sole focus is managing sensitive data. There are also good reasons why the U.S. Department of Homeland Security identified our DMS as Critical National Infrastructure, and why the U.S. Federal Trade Commission is writing new data management regulations that will apply to the automobile industry.

The DMS mission is complex; the data we manage is vast and sensitive. Thousands of dealerships and millions of consumers need to know that we are getting it right.

We don't think that HB 3152 gets it right, and therefore we urge you to oppose it.

Thank you.