Testimony of Mayer Grashin
Counsel, CDK Global
Oregon House Committee on Business and Labor
April 8, 2019

Chairman Barker and Members of the Committee:

I am Mayer Grashin, and I am pleased to speak this morning on behalf of my industry colleagues and my CDK colleagues – including more than 400 who work in our Portland office. I urge you to oppose HB 3152, which will put at risk the privacy and security of millions of Oregonians' personally identifiable and sensitive information, including credit card, driver's license and Social Security numbers.

For over 40 years, our CDK team has built the leading Dealer Management System ("DMS") in the world, securely connecting thousands of automobile, truck, marine, and RV dealers to manufacturers, banks, credit unions, warranty and insurance companies, parts suppliers, hundreds of industry and consumer-facing applications, and local governments. Our Dealer Management System has been designated a Critical National Infrastructure by the U.S. Department of Homeland Security.

We work hard to balance two competing challenges – flexible and convenient products on the one hand and protecting and securing data on the other. The marketplace tells us that we have struck the right balance, as evidenced by the many thousands of automobile dealers nationwide, including over one hundred dealers in Oregon, that license and use our products.

Some dealers disagree with our approach, but they can choose from nearly a dozen competing providers that offer different features and different approaches to data security. Every year hundreds of dealers change DMS providers.

Some dealers, however, instead of simply changing providers, are pushing the government to legislate our security policies and the features our products and services must offer. The bill before you today would require the surprising new feature of less data security and less data protection. HB 3152 will require DMS services to open hundreds or thousands of virtual back doors to unlicensed, unmonitored intruders, and thereby jeopardize the safety and security of millions of Oregonians' personally identifiable and sensitive financial data.

As you know, in the business world the default rule is that entrepreneurs backed by private capital listen to the marketplace in deciding what products to build, features to include and prices to set. Without at least some evidence of gross malfeasance within an industry—and here there is none—there is no public policy basis for legislation of this nature. I urge you to ask the right questions and review the evidence – if the proponents present any.

Supporters of this bill may claim that it does not weaken data security or privacy and may even claim that it does the opposite and strengthens data privacy. But the words of the bill say

otherwise and so do certified, credentialed and respected cybersecurity and information security professionals.

Supporters of this bill also may hint that Dealer Management Systems are selling the dealers' data or consumer data, but that is demonstrably false. Ask them for evidence.

The same supporters say they merely want to make "protected dealer data" accessible to so-called "data-integrators"— which they say is a good thing and should cause no concerns. But the bill defines "protected dealer data" as including all consumer data and all data on the Dealer Management System that is related to dealers' operations. This includes credit card numbers, Social Security numbers, driver's license numbers, names, street addresses and email addresses, and billions of data elements provided by auto manufacturers, banks and other partners that are guaranteed security by contract and that for decades have trusted our company with their data – for good reason.

Notably, supporters of this bill who criticize DMS providers' policies fail to disclose that their "data integrator" vendors have been served with cease-and-desist letters and sued several times for their unauthorized access of enterprise computer systems, violating contracts' data security provisions, accessing secure systems in violation of the federal Computer Fraud and Abuse Act, and evading technological and contractual security measures in violation of the federal Digital Millennium Copyright Act. "Data integrators" do not deserve your trust or sympathy, and they certainly should not be propped up by legislative fiat while they flagrantly break federal computer security laws.

The Committee should ask the bill's proponents if the "data integrators" have ever accessed a computer system without authorization from the system owner; ever removed consumers' personally identifiable and financial information from a computer system without the system owner's authorization; ever evaded security features for the purpose of accessing a system; or ever – even once – knowingly removed consumer data from a database or a computer system without permission of the computer system's owner or the data owner. We respectfully suggest that you will likely find truthful answers to these questions quite enlightening.

Only after asking these questions and receiving truthful answers can the Committee meaningfully weigh the risks of accepting at face-value the assertions of the bill's supporters. And only after reviewing all of the relevant materials and speaking with data security and privacy experts should the Committee decide if it really wishes to override the opinion of those experts and hundreds of contracts that govern the use of this data.

Millions of Oregonians' personally identifiable and sensitive data is on our systems. Oregon has passed numerous data breach and security bills this session. Why would you pass this bill and undermine those efforts to keep data safe and secure?

I welcome your questions.

Thank you.