Jonathan Emmanual
Reynolds and Reynolds
Testimony Before the Oregon House Business and Labor Committee
April 8, 2019

I am Jonathan Emmanual of The Reynolds and Reynolds Company. Reynolds built and maintains one of the critical computer systems that help automobile dealerships run their business.

The Reynolds Dealer Management System processes and secures proprietary automobile manufacturer data, sensitive and personally identifiable consumer data including Social Security numbers, credit card transactions, credit report data, banking data, and other business data that would be extremely valuable if it was acquired by the wrong people. To protect this data and to comply with federal and state data protection, consumer privacy and financial services laws, the Reynolds DMS has very strict access controls. This would all go to waste if HB3152 becomes law, and as a result every Oregon citizen who buys, leases, or services a car at a dealership would be at risk of their data being stolen and misused.

Do not be confused by proponents' statements that do not reflect the actual words in the bill. HB 3152 directly undermines our ability to manage and monitor our system and thereby puts sensitive and proprietary data at risk. The bill forbids us to take **any** action, technical or otherwise, to prohibit a so-called "authorized integrator" from obtaining, sharing, copying, transmitting or even selling data. The bill forbids us from insisting that these unlicensed third parties use logins and passwords to access the system. It forbids us from requiring that passwords be changed regularly or that they be difficult for hackers to guess. It requires us to give system access – more access than we offer to auto manufacturers or banks – to parties whom we have no knowledge of, no control over, and no recourse to even terminate their access if they do harm to our system or misuse the data that we are paid to protect.

Cybersecurity experts agree that the weakest point in an enterprise computer network is people – employees and consultants. The smallest mistake by an unmonitored third party accessing an enterprise network risks the integrity of the entire computing environment. We all know how computer viruses find a weak point and take down very large computing systems. If DMS integrity is breached the harm will spread – to all dealers that utilize the breached DMS, credit reporting agencies, banks that provide consumer financing, manufacturers, insurers, warranty companies, and state government titling and tax authorities.

Mr. Chairman, billions of dollars of private capital have built very secure systems that protect very valuable data. In the State of the Silicon Forest, where Intel, Amazon and our CDK colleagues build great and secure technology, I'm perplexed that legislation which is contrary to all the current trends and priorities regarding cybersecurity and consumer privacy would even be considered. If DMS providers are prohibited from taking any action to secure their system from third party access (so that dealers can hand out access at will), you are mandating that we make our systems vulnerable to cybercriminals with malicious motives. I urge you to read the words of this bill, to consider its implications carefully, and to vote "no" on its movement toward enactment.

Thank you.