

1 QUARLES & BRADY LLP  
2 Firm State Bar No. 00443100  
3 Renaissance One, Two N. Central  
4 Phoenix, AZ 85004-2391, 602-229-5200  
5 Brian A. Howie (AZ No. 026021)  
[Brian.Howie@quarles.com](mailto:Brian.Howie@quarles.com)  
6 Lauren E. Stine (AZ No. 025086)  
[Lauren.Stine@quarles.com](mailto:Lauren.Stine@quarles.com)  
7 *Attorneys for Plaintiffs*

8 SHEPPARD, MULLIN, RICHTER &  
9 HAMPTON LLP  
10 2099 Pennsylvania Ave., NW, Ste. 100  
11 Washington, DC 20006, 201-747-1900  
12 Thomas J. Dillickrath\* (DC 483710)  
[TDillickrath@sheppardmullin.com](mailto:TDillickrath@sheppardmullin.com)

13 Four Embarcadero Center, 17th Floor  
14 San Francisco, CA 94111, 415-434-9100  
15 Amar S. Naik\* (CA 307208)  
[ANaik@sheppardmullin.com](mailto:ANaik@sheppardmullin.com)  
16 Molly C. Lorenzi\* (CA 315147)  
[MLorenzi@sheppardmullin.com](mailto:MLorenzi@sheppardmullin.com)

17 GIBBS & BRUNS LLP  
18 1100 Louisiana, Ste. 5300  
19 Houston, TX 77002, 713-650-8805  
20 Aundrea K. Gulley\* (TX 24034468)  
[agulley@gibbsbruns.com](mailto:agulley@gibbsbruns.com)  
21 Denise Drake\* (TX 24092358)  
[DDrake@gibbsbruns.com](mailto:DDrake@gibbsbruns.com)  
22 *Attorneys for The Reynolds and Reynolds Co.*

MAYER BROWN LLP  
71 S. Wacker Drive  
Chicago, IL 60606  
312-782-0600  
Britt M. Miller\* (IL 6256398)  
[BMiller@mayerbrown.com](mailto:BMiller@mayerbrown.com)  
Michael A. Scodro\* (IL 6243845)  
[MScodro@mayerbrown.com](mailto:MScodro@mayerbrown.com)  
Brett E. Legner\* (IL 6256268)  
[BLegner@mayerbrown.com](mailto:BLegner@mayerbrown.com)

1999 K Street, NW  
Washington, DC 20006  
202-263-3000  
Mark W. Ryan\* (DC 359098)  
[mryan@mayerbrown.com](mailto:mryan@mayerbrown.com)  
*Attorneys for CDK Global, LLC*

*\*Pro Hac Vice Forthcoming*

23 IN THE UNITED STATES DISTRICT COURT  
24 FOR THE DISTRICT OF ARIZONA

25 CDK Global, LLC, a limited liability company,  
26 and The Reynolds and Reynolds Company, a  
corporation,

Plaintiffs,

vs.

Mark Brnovich, Attorney General of the State  
of Arizona, and John S. Halikowski, Director of  
the Arizona Department of Transportation,

Defendants.

Case No.:

**COMPLAINT**  
**(Declaratory Judgment)**

1 Plaintiffs CDK Global, LLC (“CDK”) and The Reynolds and Reynolds Company  
2 (“Reynolds”), through their undersigned attorneys, bring this complaint for declaratory and  
3 injunctive relief and in support allege as follows.

4 **INTRODUCTION**

5 1. This lawsuit challenges Arizona House Bill 2418 (the “DMS Law”), codified  
6 at §§ 28-4651 to 28-4655 of the Arizona Revised Statutes. Plaintiffs provide proprietary  
7 computer systems to automotive dealers (known as “dealer management systems” or  
8 “DMSs”). The DMS Law purports to require Plaintiffs to give third parties unfettered access  
9 to and use of Plaintiffs’ DMSs, and the sensitive customer data they store, manage, and  
10 protect, without Plaintiffs’ authorization. The law effectively interferes with Plaintiffs’  
11 established contract rights and takes Plaintiffs’ intellectual property, ultimately putting  
12 highly confidential information pertaining to Arizona consumers at great risk without any  
13 justification and in disregard of the laws and Constitution of the United States, and  
14 potentially exposing Plaintiffs to substantial criminal penalties.

15 2. The DMS Law was falsely described to legislators as a consumer-protecting  
16 data privacy measure. In fact, the DMS Law was drafted and pushed through by the Arizona  
17 Automobile Dealers Association, the top donor to the law’s sponsor in his last election. Far  
18 from protecting consumers, the DMS Law necessarily puts consumers’ data at extremely  
19 high risk by allowing unlicensed third parties—including those seeking to access, collect,  
20 and profit from selling consumer data—to access Plaintiffs’ DMSs and all of the data on  
21 those systems, and forbids Plaintiffs from taking any measures to secure those systems and  
22 data.

23 3. Rather than protecting consumers, the DMS Law is a blatant attempt by car  
24 dealers to change the terms of freely negotiated, arms-length contracts with Plaintiffs and  
25 to interfere with Plaintiffs’ contracts with other parties, for short-term economic gain and  
26 at the expense of the people of Arizona.

1 4. In committee debate on the DMS Law, Senator Eddie Farnsworth warned on  
2 the record: “I really do think that we’re walking on some thin ice here when we start to pass  
3 laws that interfere with current contracts. And quite honestly, there’s a potential  
4 unconstitutionality issue here.”

5 5. Senator Farnsworth was right: the DMS Law is preempted under the  
6 Supremacy Clause of the U.S. Constitution because it conflicts with federal law and policy.  
7 It is also void for vagueness and violates several other provisions of the Constitution: it  
8 takes private property without just compensation, interferes with contracts, unduly burdens  
9 interstate commerce, and impermissibly compels speech.

10 6. Beyond its unconstitutionality, if the DMS Law is enforced, millions of  
11 Arizonans are likely to see the private information they entrusted to auto dealers —  
12 including their driver’s license and Social Security numbers, home address, email, phone  
13 numbers, and bank or other financial information — exposed to harvesting, aggregation,  
14 and syndication by third parties who do not have the same obligations to protect data that  
15 dealers have and who often sell such data to the highest bidder.

16 7. Additionally, by giving third parties unfettered rights to introduce their  
17 computer code into the system, the DMS Law exposes DMS providers to threats caused by  
18 introducing a known security risk into a trusted network. Once in the network, a cyber-  
19 attacker could hack into other systems and cause direct financial harm to the DMS provider.

20 **BACKGROUND**

21 8. Plaintiffs CDK and Reynolds are automotive technology companies that have  
22 developed complex, advanced proprietary computer systems known as dealer management  
23 systems. Car dealerships often license DMSs to help manage accounting, sales, service,  
24 finance, payroll, and other business operations. In those contracts, the licensee dealers  
25 expressly agree that the license is limited, that they are not authorized to grant further  
26 licenses to others, and that they may not access or use the DMSs by means other than those

1 permitted by the Plaintiffs acting as licensors. Plaintiffs' DMSs process vast amounts of  
2 confidential consumer and third-party information, copyrighted or copyrightable material,  
3 and trade secrets. Such data include highly sensitive and/or proprietary material from  
4 automotive dealerships, their customers, car manufacturers, application software providers,  
5 banks, credit bureaus, other financial institutions, and the DMS providers themselves.

6 9. DMSs also securely transmit certain data to entities involved in a dealership's  
7 business operations (e.g., sending consumer data to a credit bureau for a credit check during  
8 the vehicle financing process or receiving updated parts pricing data from a car  
9 manufacturer).

10 10. CDK's and Reynolds's DMSs are secure because they must be. Numerous  
11 federal laws and regulations, as well as industry best practices, limit how data may be  
12 handled, stored, or processed on a DMS. Relevant laws include the Gramm-Leach-Bliley  
13 Act ("GLBA"), the Fair and Accurate Credit Transactions Act, the FTC's Privacy,  
14 Safeguards, and Disposal Rules, the Fair Credit Reporting Act, and the Dodd-Frank Act.  
15 Data handled, stored, or processed on a DMS is also governed by contracts with car  
16 manufacturers, financial institutions, and other third parties to whom such data is sent or  
17 received.

18 11. In light of these statutory and contractual obligations, as well as the trust that  
19 Plaintiffs' customers and other members of the automotive industry place in their DMSs,  
20 Plaintiffs (1) deploy strict authorization and authentication measures to control access to  
21 their proprietary systems; (2) require third parties to go through integration testing  
22 procedures; and (3) follow strict integration specifications. In these ways, Plaintiffs  
23 maintain data integrity and diligently defend their DMSs against cyber-attack, corruption,  
24 and breach.

25 12. At great expense, Plaintiffs have developed technologically sophisticated  
26 security measures to prevent unlicensed and unauthorized access to their DMSs. Plaintiffs

1 have also developed their own proprietary processes for securely handling data  
2 communications between dealerships, car manufacturers, and other third parties involved  
3 in a dealership's business operations. Plaintiffs and other DMS providers compete with each  
4 other over the security, functionality, and performance of their system designs, and the  
5 ability to provide strong security is a competitive advantage.

6 13. The DMS Law takes away Plaintiffs' control over their proprietary systems,  
7 however, effectively requiring all DMS providers to use non-secure methods of system  
8 access and data transmittal by eliminating the rigorous security and operational measures  
9 Plaintiffs have spent millions of dollars and a massive number of human-hours to develop  
10 and maintain.

11 14. Specifically, the DMS Law forces Plaintiffs to provide unlicensed third  
12 parties (whether they be automotive marketing firms, other service providers, or malicious  
13 hackers) with free and unfettered access to Plaintiffs' proprietary systems. The *only*  
14 restriction placed on this access is that it be at the request of a dealership employee.

15 15. In addition to DMSs, many dealers use software applications provided by  
16 third parties. In some instances, the dealers would like those third-party application  
17 providers to leverage DMS data and processes, which may include accessing data stored on  
18 the DMS or writing data back to it. Both Plaintiffs provide robust, monitored means for  
19 those legitimate providers to do so. But there are also third parties that attempt to gain  
20 unauthorized access to the DMS for several different purposes. Some want to write data  
21 back to the system. Some want to extract data from the system. And some of these data  
22 extractors are so-called "syndicators," who have historically attempted to access Plaintiffs'  
23 DMSs without authorization to hijack consumer and proprietary data and sell it to other  
24 parties without Plaintiffs' permission (in many cases, without dealer or consumer  
25 knowledge). The DMS Law forbids Plaintiffs from taking any measures to secure their  
26 systems or limit the data that a third party can access, extract, or modify on the DMS.

1           16. If the DMS Law is enforced, it will place all consumer and proprietary data  
2 stored or processed on any DMS at great risk. Consumers will face a significantly increased  
3 threat of identity theft every time they buy, lease, or service a vehicle from an Arizona  
4 dealer. The same will be true of anyone who has purchased, leased, or serviced a car from  
5 an Arizona dealer in recent years.

6           17. In short, the DMS Law requires Plaintiffs to tear down their security walls  
7 and build a back door to Plaintiffs' DMSs, giving data pirates and cyberthieves free license  
8 to jump unimpeded into the pool of data provided by Arizona consumers.

9           18. Further, by forcing Plaintiffs to open their secure proprietary systems to  
10 unlicensed third parties, the DMS Law eviscerates Plaintiffs' intellectual property rights in  
11 their proprietary computer systems, undercutting the economic incentive for them to  
12 develop and innovate on the systems capable of helping Arizona dealers manage their  
13 businesses while securing Arizona consumers' highly sensitive data.

14           19. The DMS Law is problematic in numerous other respects. It requires  
15 Plaintiffs and other DMS providers to write new computer code allowing third parties to  
16 access and write data back to the DMSs and forbids these providers from charging for that  
17 work. It eliminates the many approaches currently used by DMS providers like Reynolds  
18 and CDK to enhance system access and security within the automotive software industry  
19 and forbids DMS providers from securing their systems. Equally important, the law creates  
20 a gaping vulnerability in DMSs that impacts thousands of dealer licensees and tens of  
21 millions of consumers within and without Arizona's borders.

22           20. The DMS Law conflicts with the federal laws that keep Arizona consumers'  
23 (including car buyers') personal information safe. It conflicts with the federal laws that  
24 protect Plaintiffs' property interests in, and rights to exclude users from, their DMSs. And  
25 it substantially impairs Plaintiffs' existing contracts with dealers; takes Plaintiffs' property  
26 for no public use and without compensation; carves out special rules for Arizona car

1 dealerships that unreasonably burden interstate commerce; and violates Plaintiffs' right to  
2 free speech by compelling them to draft and implement computer code and exchange  
3 information with third parties.

4 21. At the same time, the DMS Law is fatally vague, and exposes DMS providers,  
5 including Plaintiffs, to criminal penalties, including fines of up to \$16,000 per day. The  
6 DMS Law will be added to Title 28 of the Arizona Revised Statutes. Section 28-121(A)  
7 states that a person who violates a provision of Title 28 or fails or refuses to do or perform  
8 an act or thing required by Title 28 is guilty of a Class 2 misdemeanor. For corporate entities  
9 like Plaintiffs, the fine for a Class 2 misdemeanor is up to \$10,000 "per offense." In addition,  
10 Section 28-121(C) provides that violations of Title 28 are subject to certain statutory  
11 surcharges, which are levied on top of the base fine. Together, these statutory provisions  
12 mean that a DMS provider, like Plaintiffs, is subject to fines of up to \$16,000 per offense.

13 22. Because the onerous requirements that the DMS Law places on DMS  
14 providers are facially invalid under federal and state law, the Court should declare the law  
15 void and enjoin its enforcement against Plaintiffs.

16 **THE PARTIES**

17 23. Plaintiff CDK Global, LLC is a Delaware limited liability company with its  
18 corporate headquarters and principal place of business at 1950 Hassell Road, Hoffman  
19 Estates, Illinois 60169. CDK is a global provider of integrated information technology and  
20 digital marketing solutions to the automotive retail industry.

21 24. The automotive data ecosystem that CDK supports is massive, with tens of  
22 thousands of installations of approved vendor applications and millions of transactions  
23 every day, supporting hundreds of billions of dollars in commerce each year. In light of the  
24 size, scope, and importance of its network to the American economy, the Department of  
25 Homeland Security has designated CDK's DMS a Critical National Infrastructure "so vital  
26



1 to the United States that [its] incapacitation would have a debilitating effect on security  
2 [and] national economic security.”

3 25. CDK has made substantial investments to build out and support its network  
4 of product and Software as a Service (SaaS) offerings. Over the last four years alone, CDK  
5 has spent more than \$100 million researching, developing, and deploying new and enhanced  
6 products for its customers.

7 26. Plaintiff The Reynolds and Reynolds Company is a privately held Ohio  
8 corporation with its corporate headquarters at One Reynolds Way, Kettering, Ohio 45430.

9 27. Reynolds developed, maintains, owns, and operates a proprietary enterprise  
10 computer system that car dealerships license to manage their businesses. The system has  
11 hundreds of millions of lines of natively developed source code deployed in Reynolds’s  
12 software programs.

13 28. Reynolds’s ongoing development of its DMS has produced a single system  
14 capable of supporting data communications between and among licensed dealerships, new  
15 car manufacturers, financial institutions, and automotive application software.

16 29. Defendant Mark Brnovich is the Attorney General of Arizona and in that  
17 position is the chief law enforcement officer of the State and has responsibility for enforcing  
18 the DMS Law. Specifically, pursuant to A.R.S. § 28-333, Attorney General Brnovich “shall  
19 prosecute and defend in the name of this state all actions necessary to carry out” Title 28 of  
20 the Arizona Revised Statutes (to which the DMS Law will be added). Attorney General  
21 Brnovich is sued in his official capacity only.

22 30. Defendant John S. Halikowski is the Director of the Arizona Department of  
23 Transportation and in that position has the authority to supervise and regulate dealers,  
24 manufacturers, distributors, and other entities. Defendant Halikowski is sued in his official  
25 capacity only. Defendant Brnovich and Defendant Halikowski are referred to collectively  
26 as “Defendants.”



1 **JURISDICTION AND VENUE**

2 31. This Court has subject matter jurisdiction over Plaintiffs' claims pursuant to  
3 28 U.S.C. §§ 1331, and 2201(a). There is federal question jurisdiction under 28 U.S.C.  
4 § 1331 because Plaintiffs allege violations of the federal Constitution. Plaintiffs seek a  
5 declaration of their rights pursuant to the Federal Declaratory Judgment Act, 28 U.S.C.  
6 § 2201, over which there is an actual controversy after the enactment of the DMS Law.

7 32. This Court has personal jurisdiction over Defendants because (a) they are  
8 located in the District in which this action was filed; and (b) many of the actions giving rise  
9 to these claims occurred in and/or were directed from this District.

10 33. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c).

11 **FACTUAL ALLEGATIONS**

12 34. DMSs are proprietary systems licensed to end users (i.e., car dealerships)  
13 based on contract terms such as a limited license, with fees based on features, functionality,  
14 and number of users. DMSs run hundreds of millions of lines of computer code and  
15 incorporate valuable patents, copyrights, trade secrets, and other intellectual property. They  
16 also store and process sensitive consumer, financial, and proprietary data. Many companies,  
17 including CDK and Reynolds, develop, own, operate, and license DMSs.

18 35. DMSs are distributed computer systems that operate in interstate commerce  
19 across state lines. For example, an Arizona dealership licensing a Reynolds DMS could  
20 have a DMS server that resides on-site at its dealership and connects with Reynolds data  
21 centers in Texas and/or Ohio, automakers in Michigan, and software application vendors in  
22 Georgia, Florida, and/or California. In addition, many dealership groups have multi-state,  
23 regional, or national operations and enter into a single set of contracts with a DMS provider  
24 to license the DMS across some or all of their operations.

25 36. CDK and Reynolds, like many other DMS providers, deploy strict access  
26 controls on their systems to comply with both federal and state data security and privacy

1 laws and their contracts with dealers, and to manage the security, privacy, and performance  
2 of their proprietary enterprise computer systems. Typically, only dealership employees may  
3 use DMS login credentials to access the DMS. In accordance with the DMS contract and  
4 their own obligations under federal law, these dealership employees cannot share these  
5 credentials with any non-dealership employee or use the DMS for purposes other than the  
6 dealership's business. Additionally, the DMS contracts prevent automated access to the  
7 DMS unless authorized by the DMS provider.

8 37. Although CDK's DMS is different than Reynolds's, the DMS Law affects  
9 both companies' DMSs in a similar manner. Both companies' DMSs provide licensees with  
10 the option to allow automakers (also known as Original Equipment Manufacturers or  
11 "OEMs"), lenders, credit bureaus, application providers, and other third parties to  
12 interoperate with their respective DMSs through system interfaces that securely manage the  
13 flow of data. Each of those interfaces is also established and governed by its own licensing  
14 agreements.

15 **A. CDK's DMS**

16 38. CDK's DMS offering to car dealers consists primarily of two products that  
17 provide dealers with proprietary software tools and resources used to manage core aspects  
18 of their businesses. CDK currently licenses its DMS to more than 30,000 dealerships around  
19 the world and approximately 8,000 new car dealerships in North America. CDK annually  
20 processes 2.5% of the U.S. gross domestic product (approximately \$500 billion) through its  
21 software solutions.

22 39. CDK has invested hundreds of millions of dollars to develop the hardware  
23 and software components of its DMS over decades. CDK's DMS contains, and consists of,  
24 valuable intellectual property including patented technologies, proprietary software  
25 elements and programs created by CDK (including software programs eligible for  
26 protection by the copyright laws), and proprietary data collections, which are accessible

1 through the DMS. Dealers that license DMS services from CDK receive a personal, non-  
2 transferable software license to use CDK's DMS in accordance with the terms and  
3 conditions of their agreements.

4 40. CDK's terminal program, which runs on dealer computers, is an original and  
5 independent work created and licensed by CDK. It consists of original and distinct elements,  
6 including its source and object code; distinctive screen layouts; graphical content; text;  
7 arrangement, organization, and display of information; dynamic user experience; and secure  
8 connectivity between dealer endpoints and CDK's networks.

9 41. In addition to its core functionalities, the CDK DMS processes and/or stores  
10 voluminous amounts of highly sensitive data, including financial statements, accounting  
11 data, payroll information, sales figures, inventory, parts data, warranty information,  
12 appointment records, service and repair records, vehicle information, customer personal  
13 identifiable information, proprietary intellectual property, and proprietary data belonging to  
14 CDK and third parties, including the data described below.

15 42. Such data belongs to several types of entities. Some data, such as prices and  
16 part numbers for replacement parts, labor rates, and rebate, incentive, and warranty  
17 information is proprietary to OEMs such as General Motors, Ford, and Subaru. Other data  
18 in or processed by CDK's DMS is proprietary to third-party service providers, such as credit  
19 reporting bureaus like Equifax, Experian and TransUnion. Still other data in the DMS is  
20 CDK's own proprietary, copyrightable data, including forms, accounting rules, tax tables,  
21 service pricing guides, and proprietary tools and data compilations. And while some data  
22 "belongs" to the dealers, in the sense that dealers enter the data into the system, that use  
23 CDK's DMS, much of that is consumer data. Access to third-party and CDK proprietary  
24 information in the DMS is permitted for licensed DMS customers, but CDK is prohibited  
25 by contract from sharing much of this information with any other third parties.

26

1           **B. Reynolds's DMS**

2           43. Reynolds introduced its first computerized DMS, called "ERA," in the late  
3 1980s. In 2006, Reynolds merged operations with Dealer Computer Services, Inc., which  
4 had developed a separate DMS product in the 1980s now known as POWER. Reynolds  
5 continues to offer both POWER and ERA (collectively, the "Reynolds DMS").

6           44. The Reynolds DMS is an integrated system of hardware and software  
7 components distributed to over 5,000 franchised new car dealerships in North America,  
8 including: dealer-side or hosted servers; operating systems, segregated databases, and  
9 application layers on the servers; secured interfaces between the servers and the dealer's  
10 computers; end-user application software on the dealer's computers; secure data  
11 connections from the servers to the data centers and centralized processing facilities;  
12 security measures including encryption, access monitoring, and password complexity  
13 requirements; and network and system components including Virtual Local Area Networks,  
14 Wide Area Networks, print servers, and software.

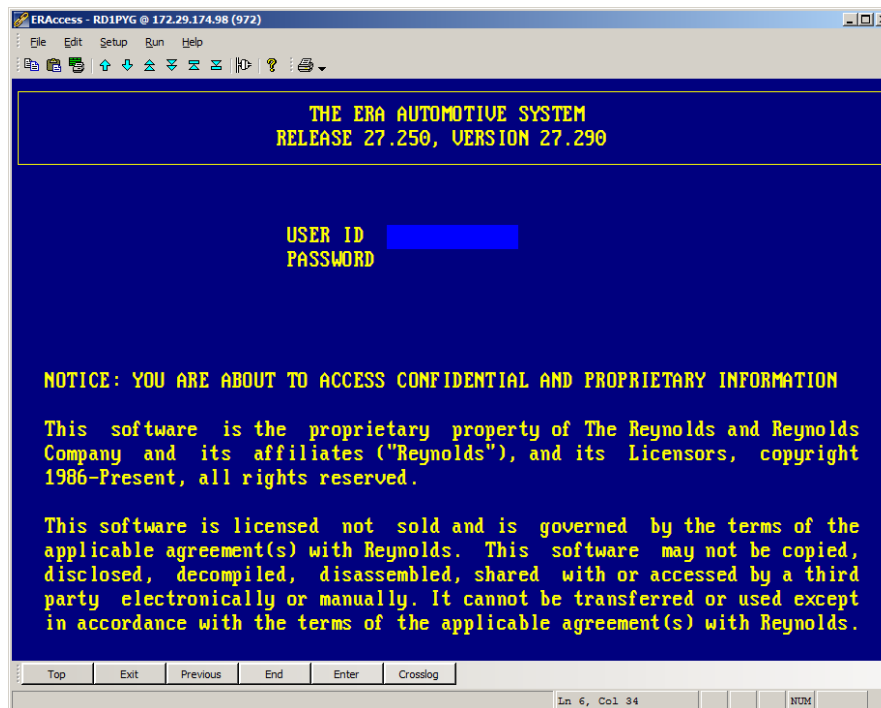
15           45. These components allow retail automotive dealers to manage their  
16 inventories, bookkeeping and accounting, customer contacts, financial and insurance  
17 information, transactional details, government reporting and compliance requirements,  
18 human resources files, and many other materials involved in managing an auto dealership.  
19 Each Reynolds DMS is custom built to provide the hardware and software components that  
20 an individual dealership needs to maximize performance.

21           46. Reynolds's customers depend upon the DMS to process highly sensitive  
22 and/or proprietary data, including consumer data; dealer operational and business data;  
23 OEM data; credit and financial data; Reynolds's proprietary data; and data licensed from  
24 third parties. These categories of information are protected by federal data security and  
25 privacy laws, as well as contracts governing data access.

26

1 47. Over the course of two decades, Reynolds invested well over half a billion  
2 dollars and millions of human-hours in building, securing, and maintaining the proprietary  
3 design and interaction of the components of its DMS platform in the face of ever-evolving  
4 technology. Reynolds continues to invest in its DMS platform.

5 48. The Reynolds DMS software program that runs on dealer computers is an  
6 original copyrighted work. Among the many significant original elements of the program  
7 are its source and object code; distinctive screen layouts; graphical content; text;  
8 arrangement, organization, and display of information; and dynamic user experience. Every  
9 time a user opens the Reynolds DMS software program, it displays a notice stating that the  
10 program is Reynolds's copyrighted, confidential, and proprietary property:



23 49. It is impossible for a user to access or use the Reynolds DMS without running  
24 (and thereby copying) Reynolds's copyrighted DMS software programs. Reynolds does not  
25 allow any dealer, application provider, or other third party to access the Reynolds DMS  
26 without a valid license or express authorization.

1           50. Reynolds's DMS is a custom product and is offered pursuant to highly  
2 negotiated license agreements with dealers. Though the products, services, and terms differ  
3 widely among dealers, all dealers that license a Reynolds DMS agree that only dealership  
4 employees may access Reynolds's proprietary DMS. Dealers further agree not to connect  
5 any third-party software to their Reynolds DMS. Reynolds's prohibition on third-party  
6 access to its DMS has been widely known in the automotive industry for at least a decade.

7           **C. Security Features to Control Access to DMSs**

8           51. Plaintiffs employ a number of technologically advanced security features to  
9 protect the data and functionality of their DMSs and guard against unauthorized access. As  
10 detailed below, these features include password protections, login prompts, and contractual  
11 security provisions. The following are some examples. Plaintiffs are continuously  
12 introducing new security measures to combat new methods of attempted unauthorized  
13 access, and Plaintiffs cannot disclose all of their security measures to the public.

14           **1. CDK Security Controls**

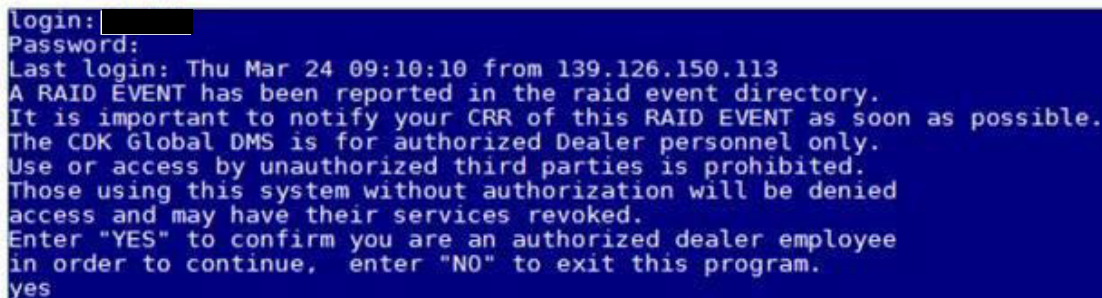
15           52. For example, among CDK's many security measures, its DMS is password  
16 protected. To gain access, each dealership employee must use that employee's individual  
17 login credentials.

18           53. Typically, at least one employee at each dealership using CDK's DMS has  
19 "system administrator"-level access privileges. A dealership employee has compared  
20 having system administrator-level access to possessing "the keys to the kingdom." Users  
21 with system administrator-level privileges may create new accounts (and corresponding  
22 login credentials) for other dealership employees. These users also have the ability to define  
23 the data and functions each employee may access within CDK's DMS by creating and  
24 assigning the employees different "roles." In other words, each user has access to the DMS  
25 commensurate with the access privileges assigned to his or her login credentials.

26

1           54. Data maintained in CDK's DMS is used in four primary application areas:  
2 Accounting, Finance & Insurance Sales, Parts, and Service. The login credentials that  
3 dealerships create for their employees can be configured to allow access to all four functions  
4 or only specific ones. Login credentials also may be configured to run reports, search data,  
5 and modify data as appropriate. Upon information and belief, car dealerships have in the  
6 past provided login credentials to third parties, that thereby gained unauthorized, automated  
7 access to CDK's DMS, and those credentials often allowed general access to most or all  
8 application areas. This access has allowed unauthorized third parties to install programs on  
9 the system, creating technological issues during system upgrades and causing additional  
10 security concerns.

11           55. CDK has implemented security features in addition to password protection.  
12 In early 2016, CDK created a login prompt, depicted below, requiring users to certify that  
13 they were an "authorized dealer employee" before they could access CDK's DMS.



```
login: [REDACTED]
Password:
Last login: Thu Mar 24 09:10:10 from 139.126.150.113
A RAID EVENT has been reported in the raid event directory.
It is important to notify your CRR of this RAID EVENT as soon as possible.
The CDK Global DMS is for authorized Dealer personnel only.
Use or access by unauthorized third parties is prohibited.
Those using this system without authorization will be denied
access and may have their services revoked.
Enter "YES" to confirm you are an authorized dealer employee
in order to continue, enter "NO" to exit this program.
yes
```

14  
15  
16  
17  
18  
19           56. Further, in November 2017, CDK began introducing a "CAPTCHA" control  
20 for particular login credentials that CDK suspected third parties of using to facilitate  
21 unauthorized access to its DMS. CAPTCHA (an acronym for "completely automated public  
22 Turing test to tell computers and humans apart") controls are simple tests designed to tell  
23 whether a request for access is coming from a human or a machine impersonating a human.  
24 These controls are designed specifically to prevent access to computers through automated  
25 means.

26



1           57. The CAPTCHA used by CDK states that “[o]nly dealer personnel are  
2 authorized to use the CDK Global DMS. Use or access by unauthorized third parties is  
3 strictly prohibited and violates the contractual terms on which CDK licenses its software  
4 and services. Machine/automated access . . . or issuing of user names and passwords for  
5 third party use is considered non-authorized access.” The CAPTCHA then requires the user  
6 to identify a word or series of letters and numbers to “confirm you are an authorized dealer  
7 employee” before allowing the user to log into the CDK DMS.

8           58. As another example of its security innovations, CDK has virtualized the entire  
9 DMS environment. This virtualized environment enables CDK to manage the system more  
10 easily.

11           59. CDK’s contracts also impose contractual security. For example, partner  
12 vendors agree not to access or retrieve data from or write it to a CDK system using  
13 unapproved methods. Partner vendors also represent and warrant that they will maintain  
14 appropriate security measures regarding sensitive information.

## 15                   **2. Reynolds Security Controls**

16           60. Protecting the integrity and security of the Reynolds platform and the  
17 sensitive data it contains is a paramount concern for both Reynolds and its customers.  
18 Reynolds’s DMS includes multiple protections designed to exclude hackers, prevent  
19 automated scripts from encumbering system resources, and ensure that only properly  
20 licensed dealership employees can access and use the system.

21           61. Reynolds strictly controls and manages system access to and interoperability  
22 with its DMS through a series of technological security measures that manage the array of  
23 sensitive consumer, financial, and proprietary data flowing through the Reynolds network.

24           62. First, the Reynolds DMS can only be accessed by dealership employees  
25 through Reynolds’s proprietary terminal software. These software programs are known as  
26

1 ERA-Ignite (the current program) and ERAccess (the legacy program). Both are  
2 copyrighted. Both also contain extensive security features.

3 63. Dealership employees accessing the DMS through these programs must first  
4 answer a login prompt requiring the user to enter a valid username and password to access  
5 the system. Reynolds links each set of authorized login credentials to a dealership employee.  
6 Each set of credentials also has individualized access permissions within the DMS, based  
7 on the employee's role at the dealership. For example, a salesperson will generally have  
8 access to different DMS functionality than a service advisor or dealership manager. These  
9 controls prevent unauthorized access and mitigate the risk of errors by limiting the  
10 employee's access to the DMS to that required by the scope of the employee's duties.

11 64. Reynolds deploys CAPTCHA controls to protect the Reynolds DMS from  
12 unauthorized automated software programs attempting to access data. After logging in, a  
13 dealership employee must pass through a CAPTCHA control to access the Reynolds DMS  
14 data-exporting functions. It is impossible for a dealer-user to access these and other portions  
15 of the Reynolds DMS platform without first passing the CAPTCHA control. Reynolds also  
16 deploys CAPTCHA control prompts when Reynolds security measures determine that a set  
17 of login credentials is being used in a manner inconsistent with authorized access.

18 65. Reynolds's software also monitors all user credentials to look for suspicious  
19 patterns and potential security threats. Specifically, Reynolds's Suspicious User ID  
20 heuristic software monitors a variety of factors that differentiate automated scripts and bots  
21 from bona fide human users, including keystroke speed, keystroke pattern, source of  
22 keystroke signals (physical keyboard versus virtual keyboard), and the volume and timing  
23 of data requests. If the monitoring software determines that, based on a number of these  
24 factors, users are suspicious, then the system deactivation protocols are triggered.

25 66. Reynolds has also built extensive security features into how it interoperates  
26 with third parties. The Reynolds Integration Hub is specifically designed to provide bespoke

1 system integration to facilitate data communications between the Reynolds DMS and  
2 OEMs, application providers, and financial institutions. Reynolds continually monitors the  
3 various data flows through the Hub for errors and other alerts. The Reynolds Integration  
4 Hub includes a “journaling” function that protects against corruption risk from automated  
5 “write-backs” by third-party vendor software into DMS databases. Such automated data  
6 pushes involve the creation of more entries and transactions than an actual individual human  
7 user could possibly produce and can push thousands of erroneous entries into the DMS  
8 within minutes. The erroneous data entries resulting from these automated data pushes  
9 occurring in one part of the DMS can propagate across other DMS functionalities,  
10 effectively paralyzing one or even multiple systems. Reynolds’s proprietary journaling  
11 technology allows Reynolds to audit and trace the effects of malfunctioning vendor  
12 software.

13 67. Reynolds’s license and interface agreements impose contractual security  
14 obligations on its third-party providers and vendors through the Reynolds Certified  
15 Interface program. Those application providers are prohibited from using unapproved  
16 methods to access the Reynolds DMS; are required to notify Reynolds promptly in the event  
17 of a security breach; and must warrant to Reynolds that they have dealer permission and  
18 will comply with data security and privacy laws. Reynolds requires vendors to include terms  
19 in their End User License Agreements with dealers detailing appropriate safeguards  
20 designed to protect sensitive customer information. Reynolds reserves the right to—and  
21 does—audit these vendor-partners to ensure compliance.

### 22 3. These Security Controls Are an Important Part of the DMSs

23 68. The development and implementation of security controls such as CAPTCHA  
24 screens and contractual obligations are vital to keep private data, including the enormous  
25 amount of private personal data stored in the DMSs, out of the hands of hackers and other  
26 unauthorized parties. But the DMS Law greatly restricts, if not entirely prevents, the

1 effective use of such controls by broadly prohibiting DMS providers such as Plaintiffs from  
2 employing any “technical means” to restrict access by third parties (including malicious  
3 hackers).

4 **D. Federal Law Protecting DMS Providers’ Property**

5 69. The Copyright Act states that “[a]nyone who violates any of the exclusive  
6 rights of the copyright owner . . . is an infringer of the copyright or right of the author.” 17  
7 U.S.C. § 501(a). The Act enables any “legal or beneficial owner of an exclusive right under  
8 a copyright . . . to institute an action for any infringement of that particular right committed  
9 while he or she is the owner of it.” 17 U.S.C. § 501(b).

10 70. The Digital Millennium Copyright Act (“DMCA”) provides that no “person  
11 shall circumvent a technological measure that effectively controls access to a work  
12 protected under this title.” 17 U.S.C. § 1201(a)(1)(A). It also provides that “[n]o person  
13 shall manufacture, import, offer to the public, provide, or otherwise traffic in any  
14 technology, product, service, device, component, or part thereof, that . . . is primarily  
15 designed or produced for the purpose of circumventing a technological measure that  
16 effectively controls access to a work protected under this title.” *Id.* § 1201(a)(2)(A). The  
17 DMCA further states that “[n]o person shall manufacture, import, offer to the public,  
18 provide, or otherwise traffic in any technology, product, service, device, component, or part  
19 thereof, that is primarily designed or produced for the purpose of circumventing protection  
20 afforded by a technological measure that effectively protects a right of a copyright owner  
21 under this title in a work or a portion thereof.” *Id.* § 1201(b)(1)(A). To enforce these  
22 prohibitions, the DMCA not only provides for criminal sanctions, *see id.* § 1204, but also  
23 gives copyright owners a private right of action against those who unlawfully access their  
24 copyrighted works, *see id.* § 1203 (“Any person injured by a violation of section 1201 or  
25 1202 may bring a civil action in an appropriate United States district court for such  
26 violation.”).

1           71. Software developed and licensed by DMS providers is subject to copyright  
2 protections. For example, Reynolds has registered copyrights for multiple versions of its  
3 DMS terminal software program. (Registration Nos. TX 7-586-896; TX 7-586-863; TX 8-  
4 538-825; and TX 8-538-541). Any unlicensed use of that DMS software (or use exceeding  
5 the terms of the license between a DMS provider and an end user such as a car dealership)  
6 infringes upon those copyrights.

7           72. Attempts by any third party to bypass, avoid, disable, deactivate, or impair  
8 DMS access-control measures by misappropriating login credentials, providing access to  
9 unlicensed third parties, or circumventing security tools such as CAPTCHA, violate  
10 § 1201(a)(1)(A)'s prohibition on circumvention of a technological measure that effectively  
11 controls access to a work protected by the Copyright Act and DMCA.

12           73. The Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836, *et seq.*, protects  
13 owners of trade secrets from misappropriation by third parties. Under the DTSA, owners of  
14 trade secrets have a federally guaranteed right to exclude others from their trade secrets.  
15 Under this law, permission to use or access a trade secret must come from the owner of that  
16 intellectual property.

17           74. The Computer Fraud and Abuse Act ("CFAA") provides that "[w]hoever . . .  
18 intentionally accesses a computer without authorization or exceeds authorized access, and  
19 thereby obtains . . . information from any protected computer," is subject to both criminal  
20 and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.*  
21 § 1030(g) (civil damages and injunctive relief). This statute also provides a private cause of  
22 action for "compensatory damages and injunctive relief or other equitable relief" to anyone  
23 who suffers at least \$5,000 in damage or loss in any one-year period "by reason of a  
24 violation" of its terms. *Id.* § 1030(g); *see id.* § 1030(c)(4)(A)(i)(I).

25           75. A DMS is a "computer" within the meaning of the CFAA, which defines that  
26 term to include not only computing devices but also "any data storage facility or

1 communications facility directly related to or operating in conjunction with such device.”  
2 *Id.* § 1030(e)(1). A DMS also is a “protected computer” within the statute’s meaning  
3 because it is used in and affects interstate and foreign commerce and communications. *See*  
4 *id.* § 1030(e)(2)(B).

5 76. Pursuant to the CFAA, the authorization required for lawful access to a  
6 computer system such as a DMS must come from the system’s owners, not from its users.  
7 Any access to a computer system without or exceeding the computer system owner’s  
8 authorization violates the statute.

9 **E. Federal Law Governing How Dealers and DMS Providers Must Secure**  
10 **Consumer Data**

11 77. The Gramm-Leach-Bliley Act (“GLBA”) requires “that each financial  
12 institution has an affirmative and continuing obligation to respect the privacy of its  
13 customers and to protect the security and confidentiality of those customers’ nonpublic  
14 personal information.” 15 U.S.C. § 6801(a).

15 78. In furtherance of this policy, the law requires federal agencies to: “establish  
16 appropriate standards for the financial institutions subject to their jurisdiction relating to  
17 administrative, technical, and physical safeguards—(1) to insure the security and  
18 confidentiality of customer records and information; (2) to protect against any anticipated  
19 threats or hazards to the security or integrity of such records; and (3) to protect against  
20 unauthorized access to or use of such records or information which could result in  
21 substantial harm or inconvenience to any customer.” *Id.* § 6801(b).

22 79. The GLBA defines financial institutions as “any institution the business of  
23 which is engaging in financial activities . . . .” *Id.* § 6809(3)(A); *see also id.* 12 U.S.C.  
24 § 1843(k) (defining “financial activities”); *id.* § 1843(k)(4) (describing “activities that are  
25 financial in nature”).

26

1           80. The GLBA defines the term “nonpublic personal information” as “personally  
2 identifiable financial information—(i) provided by a consumer to a financial institution; (ii)  
3 resulting from any transaction with the consumer or any service performed for the  
4 consumer; or (iii) otherwise obtained by the financial institution.” 15 U.S.C. § 6809(4)(A).

5           81. The Federal Trade Commission circulated the Safeguards Rule, which  
6 implements 15 U.S.C. § 6801(b), in May 2002. The Rule became effective on May 23,  
7 2003. *See* 16 CFR Part 314. It requires financial institutions to protect the security,  
8 confidentiality, and integrity of customer information by developing, implementing, and  
9 maintaining a comprehensive information security program that contains administrative,  
10 technical, and physical safeguards that are appropriate to the financial institution’s size and  
11 complexity, the nature and scope of its activities, and the sensitivity of the customer  
12 information at issue. *Id.* § 314.3. The Rule requires financial institutions to have reasonable  
13 policies and procedures to ensure the security and confidentiality of customer information  
14 and to detect, prevent, and respond to attacks, intrusions, or other system failures. *Id.*  
15 § 314.4(b). In addition to developing their own safeguards, companies covered by the Rule  
16 are responsible for taking steps to ensure that their affiliates and service providers safeguard  
17 customer information in their care. *Id.* § 314.4(d).

18           82. Federal agencies have recognized that automobile dealerships are financial  
19 institutions under the GLBA. As such, dealers and DMS providers must implement the  
20 privacy and security mandates of the GLBA.

21           83. The GLBA further provides that state law may not be inconsistent with the  
22 GLBA. *See* 15 U.S.C. § 6807.

#### 23           **F. The Contracts Between Plaintiffs and Dealers**

24           84. Plaintiffs enter into contracts licensing their DMSs to automotive dealerships  
25 throughout the country. Those contracts are freely negotiated, arms-length transactions. The  
26



1 contracts contain detailed provisions setting forth Plaintiffs' exclusive rights to control  
2 third-party access to their proprietary DMS systems.

3 **1. CDK's Master Service Agreements**

4 85. CDK has entered into Master Service Agreements with approximately 200  
5 new car dealerships in Arizona. These Agreements expressly prohibit the dealerships from  
6 allowing third parties to access CDK's DMS without CDK's authorization: "Client shall  
7 not allow access to [the CDK DMS] by any third parties except as otherwise permitted by  
8 this Agreement." MSA § 4(D).

9 86. In addition, each CDK dealer agrees, among other things, that it will only use  
10 CDK's software "for its own internal business purposes and will not sell or otherwise  
11 provide, directly or indirectly, any of the Products or Services, or any portion thereof, to  
12 any third party," *id.* § 4(B), and that it will "treat as confidential and will not disclose or  
13 otherwise make available any of the [CDK] Products and Services (including, without  
14 limitation, screen displays or user documentation) or any trade secrets, processes,  
15 proprietary data, information, or documentation related thereto . . . in any form, to any  
16 person other than employees of [the dealer] with a need to know," *id.* § 4(D). Each dealer  
17 also acknowledges that notwithstanding its license to use the CDK DMS, the DMS remains  
18 at all times "the exclusive and confidential property of [CDK]." *Id.* § 4(A).

19 87. Additionally, CDK's Master Service Agreement independently prohibits  
20 "ANY THIRD PARTY SOFTWARE TO ACCESS THE [CDK] PRODUCTS AND  
21 SERVICES EXCEPT AS OTHERWISE PERMITTED BY THIS AGREEMENT." *Id.* §  
22 4(B). This language has remained substantially unchanged in every version of the Master  
23 Service Agreement since approximately 2010.

24 88. In fact, every version of CDK's standard Master Service Agreement since at  
25 least 1994 has expressly prohibited dealers from permitting unauthorized third parties to  
26 access the dealers' licensed DMS.

1           89. In return, CDK agrees that, “to the extent it is a Service Provider to [the  
2 dealer] under the [Graham-Leach-Bliley Act’s] Safeguards Rule,” CDK will “implement  
3 and maintain appropriate safeguards as CDK may determine to be reasonably necessary to  
4 protect the confidentiality of Customer Information provided [by the dealer] to CDK  
5 pursuant to the terms of this Agreement and in CDK’s possession and control.” *Id.* § 5(F).

## 6                           **2. Reynolds’s Dealer Agreements**

7           90. Reynolds licenses its DMS to its 85 car dealerships in Arizona under a set of  
8 terms and conditions designed to protect its system’s functional integrity and security,  
9 safeguard Reynolds’s valuable intellectual property rights, and meet Reynolds’s contractual  
10 obligations to third parties. As a condition of the Reynolds Master Agreement, each  
11 Reynolds dealer agrees not to share login credentials with third parties or connect other  
12 software to the DMS. Only dealership employees are licensed to access the system.  
13 Specifically, Reynolds dealers expressly agree:

14           Reynolds (or Other Providers) retains all proprietary rights in the Licensed  
15 Matter and the Site, including copyrights, patents and trade secrets. You  
16 acknowledge that Licensed Matter [e.g., the DMS] contains Confidential  
17 Information belonging to Reynolds or Other Providers and that Licensed  
18 Matter may be subject to end user license agreements of Other Providers. You  
19 agree: (a) not to copy (other than making regular back-up copies, if permitted  
20 by us), modify, disassemble or decompile any Licensed Matter or the Site, or  
21 re-license, sublicense, rent, lease, timeshare or act as a service bureau; (b) to  
22 maintain the Licensed Matter in complete confidence; (c) *not to disclose or  
provide access to any Licensed Matter or non-public portions of the Site to  
any third party, except your employees who have a need for access to operate  
your business and who agree to comply with your obligations under this  
Section 1*; (d) to notify Reynolds immediately of any unauthorized Use or  
disclosure of Licensed Matter or your PIN or Logins (if applicable); (e) to  
cooperate with us to protect Reynolds and Other Providers’ proprietary rights  
in Licensed Matter and the Site, and (f) to comply with any end user license  
agreement of an Other Provider.

23 Reynolds Master Agreement, § 1 (emphasis added).

24           91. The Reynolds Customer Guide—which is incorporated by reference into the  
25 Master Agreement and is a part of the license agreement between Reynolds and the  
26 dealership—likewise states that the dealer “may not install Other Matter on the Equipment

1 or connect Other Matter to Licensed Matter, either directly or remotely, without  
2 [Reynolds's] prior written consent. This restriction is necessary to protect the integrity and  
3 continued functioning of the Licensed Data, Licensed Software, and the Equipment.”  
4 Customer Guide at 20. The Customer Guide defines “Other Matter” as “any software  
5 product, database, or other materials provided to you by a third party, which is capable of  
6 functioning on or with Equipment.”

7 92. The Reynolds Customer Guide further provides:

8 You expressly acknowledge that the Licensed Matter constitutes valuable  
9 proprietary property, includes confidential information and constitutes trade  
10 secrets that embody substantial creative efforts and that is valuable to  
11 Reynolds. You agree to keep confidential the Licensed Matter (including all  
licensed copies and documentation) covered under the Documents and shall  
not copy, reproduce, distribute, or in any way disseminate or allow access to  
or by third parties.

12 You expressly agree that you shall observe complete confidentiality with  
13 respect to the Licensed Matter. This agreement and requirement mean that  
14 *you shall not disclose or otherwise permit any person, firm or entity access*  
15 *to or use of the Licensed Matter.* The sole exception to this restriction is that  
16 you may disclose or grant access to the Licensed Matter to your employees  
whose employment require such access, provided that such employee is  
advised that the Licensed Matter contains proprietary property, confidential  
information and trade secrets and that each employee agrees to preserve the  
confidentiality of the Licensed Matter.

17 Reynolds Customer Guide at 21 (emphasis added).

18 93. The Reynolds Customer Guide also states that “[i]n addition to the use  
19 restrictions described in the Master Agreement and this Customer Guide, certain Licensed  
20 Data is subject to use restrictions from the Other Providers of such Licensed Data. Such  
21 Licensed Data may only be used in connection with the Reynolds System for which its use  
22 is licensed to you by us.” *Id.* at 22–23.

23 94. Reynolds's contracts with dealers also call for it to act at all times in  
24 accordance with the strictures of the GLBA. For example, the Reynolds Customer Guide  
25 states that where Reynolds is a “Service Provider” under the GLBA Safeguards Rule,  
26

1 “Reynolds will implement and maintain safeguards appropriate to protect the security,  
2 confidentiality, and integrity of your Customer Information.” Customer Guide at 10.

3 **3. These Contractual Provisions Are an Important Part of the**  
4 **Bargain Between DMS Providers and Dealers**

5 95. Dealers know and agree to these restrictions when they choose to license a  
6 DMS. Both Plaintiffs and their customer dealers negotiate the resulting licensing fees  
7 subject to those restrictions and based on the expectation that the license’s scope extends  
8 solely to dealership employees. The DMS Law abrogates these freely negotiated contractual  
9 provisions between DMS providers and dealers.

10 **G. Available Methods of Secure, Authorized Integration**

11 96. DMS providers understand that dealers sometimes seek to leverage DMS  
12 functionality for use by third-party application providers. Because unauthorized automated  
13 access poses serious risks to both the privacy, confidentiality, integrity, and availability of  
14 sensitive data, including private consumer information, and the functionality of the DMS,  
15 Plaintiffs have each developed and implemented technological methods to permit secure  
16 means of interoperating with authorized third parties.

17 **1. CDK’s Partner Program**

18 97. Introduced in 2000, CDK’s third-party access program (“Partner Program,”  
19 formerly known as 3PA) is an interface that currently provides secure managed, bi-  
20 directional integration between software applications and CDK’s DMS. Integration  
21 management includes the use of credential and access logs, which record who accessed the  
22 information, when it was accessed, and any changes made to the information. For example,  
23 the third-party marketing website TrueCar generates sales leads for dealerships. TrueCar  
24 integrates with CDK’s DMS through the Partner Program to access sales transaction data,  
25 which it uses to validate vehicle sales based on TrueCar leads. There are hundreds of other  
26

1 third-party applications that make similar use of the integration services provided through  
2 CDK's Partner Program.

3 98. Each software application vendor participating in the Partner Program enters  
4 into a written agreement with CDK granting the vendor a limited, non-transferable license  
5 to use the CDK Interface System to access, send, and/or receive certain data stored on the  
6 DMS solely to provide specific application services to CDK dealers.

7 99. CDK charges third-party participants in the Partner Program fees for the  
8 integration services it provides. These fees allow CDK to recoup its substantial investment  
9 in the Partner Program and compensate CDK for the value of its services and the intellectual  
10 property that makes secure data integration with CDK's DMS possible.

11 100. While many dealers and software vendors exchange data through the Partner  
12 Program, it is not the only way to exchange data residing on CDK's DMS. CDK's flagship  
13 DMS product, Drive, includes several reporting tools that dealers may use to compile and  
14 export their operational data, which they then can use or distribute to certain third parties.  
15 Additional reporting tools also are available to Drive users on an add-on basis.

16 101. CDK dealers can and do use these reporting tools to share data with third-  
17 party vendors instead of having those vendors access CDK's DMS through the Partner  
18 Program. The main distinction between this dealer-driven data sharing and the data  
19 integration provided by the Partner Program is the level of automation. Dealer sharing  
20 requires human intervention, while the Partner Program, once set up, is automatic. The  
21 automation and direct machine access facilitated by the Partner Program requires the extra  
22 safeguards put in place by CDK.

23 102. Plaintiffs believe that other DMS providers may permit third-party access to  
24 their systems outside of a certification program and/or without requiring those third parties  
25 to pay integration fees. CDK believes that it has a richer, more secure, product offering, but  
26 some dealers prefer a different system and are free to switch DMS providers. Many dealers

1 have left CDK in recent years and gone to another DMS provider, and many others have  
2 opted to stay or switched *to* CDK since it began taking steps, such as those described above,  
3 to manage and prevent unauthorized third-party access to its DMS.

## 4 **2. Reynolds's Certified Interface Program**

5 103. Reynolds secures interoperability with its DMS by jointly developing  
6 bespoke computer software interfaces with OEMs, application providers, credit bureaus,  
7 and other third-party partners, allowing third parties to receive data from and push data into  
8 the Reynolds DMS via dedicated, individually customized interfaces built with layers of  
9 security and data integrity safeguards. Because all interfaces run through the centralized  
10 Reynolds Integration Hub, Reynolds can secure, monitor, and support each interface with  
11 appropriate computing resources.

12 104. Reynolds tailors each partner's interface package in accordance with that  
13 partner's needs to provide service to the dealer, including communication protocols,  
14 business rules, data elements, frequency, and bi-directional capabilities. Some partners  
15 purchase multiple interface packages with different functionalities and data elements to  
16 offer different levels of service to dealers.

17 105. To handle the development of interfaces with automotive application software  
18 providers, Reynolds created the Reynolds Certified Interface Program ("RCI Program").  
19 Certified providers sign a Reynolds Interface Agreement, which requires them to describe  
20 their data use and adhere to a data use policy:

21 [Third party vendor] must describe in Exhibit A all data sets and uses of the  
22 data, which shall be subject to Reynolds' acceptance, including: the purposes  
23 of the data sets; the identities or categories of any other parties to whom  
24 [vendor] may transfer the data; and [vendor's] or any other party's uses of the  
data. Other than as specified in Exhibit A, [vendor] is prohibited from  
transferring the data to another party; or reselling the data.

25 Standard Reynolds Interface Agreement, § 6.10.

26

1           106. Reynolds and its partners in the RCI Program agree to adhere to federal data  
2 security laws and regulations: “[E]ach party agrees to comply with all legal obligations  
3 relating to the privacy and security of such ‘non-public personal information’ under the  
4 GLBA [and] the FTC regulations promulgated pursuant thereto . . . .” *Id.*, § 6.11. They also  
5 agree to take appropriate measures to prevent unauthorized access to customer data stored  
6 or processed on a DMS. *See id.*

7           107. Regardless of whether an application provider is in the RCI Program,  
8 Reynolds dealership customers can use dealer-driven data export tools to send their  
9 operational and inventory data to application providers or other third parties, as the dealer  
10 deems appropriate—including non-RCI participants. Once dealer data has been exported  
11 from the system via these standard tools, it is up to the dealer to determine whether and  
12 where to send its data. These tools, such as Dynamic Reporting (a feature that builds  
13 customized reports) or AVID (a program that configures automated vehicle inventory data  
14 reports) allow dealership employees to push data to third parties and can be scheduled to  
15 run at any time automatically.

### 16                                 **3. Plaintiffs’ Methods Ensure Data is Protected**

17           108. Both CDK and Reynolds have developed programs that enable third-party  
18 data vendors to access the DMSs in a managed, secure, and reliable way. These programs  
19 safeguard the data stored in the DMSs and ensure that third-party access will not harm the  
20 functioning of those systems. The DMS Law eviscerates these safeguards because it  
21 prohibits DMS providers from imposing fees or using technical or contractual means to  
22 restrict access to their respective systems, instead requiring them to provide unlimited  
23 access to “integrators” and any other third party authorized by dealers.

#### 24                                 **H. Hostile Access to DMSs**

25           109. Without Plaintiffs’ authorization, without paying any compensation to  
26 Plaintiffs, and in violation of several federal laws, third parties have repeatedly tried to



1 access Plaintiffs' DMSs with dealer-provided login credentials using automated machine  
2 access on interfaces designed for human use, and then writing data, extracting data, and  
3 sometimes re-selling extracted data to third-party application vendors. The DMS Law  
4 converts these unauthorized or "hostile" third parties from unauthorized data writers or  
5 extractors into "authorized integrators" and gives them the purported "right" to engage in  
6 data extraction from Plaintiffs' DMSs without Plaintiffs' permission. The DMS Law does  
7 not stop there. It also requires Plaintiffs to permit hostile third parties to create, update, and  
8 delete data on Plaintiffs' DMSs on a bulk, automated basis. The actions of these third  
9 parties—which the DMS Law demands that DMS providers allow—are the same actions  
10 that malicious criminal hackers attempt against Plaintiffs' systems every day. But the DMS  
11 Law condones this otherwise unlawful behavior, and in fact subjects Plaintiffs to liability  
12 for taking measures to protect the confidentiality, integrity, and availability of their systems  
13 from hostile attack. In addition, the DMS Law fails to contemplate potentially different  
14 forms of unauthorized access, recognizing no distinction between a hostile integrator and  
15 malicious bandits or hackers: all unauthorized access is apparently treated the same.

16       110. In the past, hostile third parties have been able to install unauthorized software  
17 directly within the DMS's core operating system by exploiting the system design (e.g.,  
18 computer hacking) or by abusing legitimate access provided to the dealer. This third-party  
19 software had not passed Plaintiffs' secure development practices and was architecturally  
20 opaque. Such activity hinders Plaintiffs' ability to respond in the event of a security incident  
21 within the DMS because such access is not monitored or logged. It also creates problems  
22 during system upgrades due to conflicts with installed software libraries and unknown code.  
23 Further, it substantially increases the impact and likelihood of corruption of files and  
24 programs within Plaintiffs' computer system. The DMS Law prevents Plaintiffs from  
25 prohibiting this practice.

26

1           111. Moreover, DMSs house both “protected dealer data” as defined by the DMS  
2 Law and other proprietary data, including Plaintiffs’ intellectual property and data licensed  
3 to Plaintiffs by OEMs and other parties. By prohibiting Plaintiffs from “tak[ing] any action  
4 by contract, technical means or otherwise to prohibit or limit a dealer’s ability to protect,  
5 store, copy, share or use protected dealer data,” the DMS Law grants third parties access to  
6 that other proprietary data as well.

7           112. And, every time a hostile third party accesses a Plaintiff DMS using dealer-  
8 provided login credentials, that third party uses valuable CDK or Reynolds intellectual  
9 property, including patented and copyrighted technologies and original software elements  
10 and programs, without Plaintiffs’ consent and in violation of the express terms of Plaintiffs’  
11 licensing agreements and system access policies.

12           113. Further, when third-party data extractors access the DMSs, they create a copy  
13 of portions of the DMS program code—as well as copies of the original and distinctive page  
14 layouts, graphical content, text, arrangement, organization, display of information, and  
15 dynamic user experience—in the Random Access Memory of the extractor’s computer.  
16 Even when third-party data extractors do not access proprietary data directly, they often  
17 access and copy data created using CDK or Reynolds and third-party proprietary forms and  
18 functions within the DMS.

19           114. Hostile third parties’ use of unauthorized, automated methods for creating,  
20 reading, updating, and deleting data places considerable strain on Plaintiffs’ DMSs,  
21 degrading system availability and consuming valuable computing resources. These parties  
22 also create serious information confidentiality and integrity concerns.

23           115. The DMS Law also defines DMSs to include “firmware,” typically low-level  
24 software used to operate wireless routers and other hardware devices. As written, the DMS  
25 Law prohibits Plaintiffs from restricting third parties from “writing data to a” DMS, which  
26 includes its firmware, and defines “protected dealer data” broadly to include material

1 potentially housed on such hardware devices. In the ordinary course, Plaintiffs do not allow  
2 *any* third parties to make changes to their DMS firmware—including dealers themselves—  
3 for numerous security and functionality reasons. Indeed, some firmware is designed to  
4 never be altered or alterable. Routers and other hardware are vulnerable attack points for  
5 any network, and the DMS Law exposes these points to a host of third parties without  
6 Plaintiffs' approval.

7 **1. Hostile Access Degrades DMS Performance**

8 116. Plaintiffs can accommodate legitimate, authorized, and managed demands for  
9 system interoperability through interfaces that facilitate the automated flow of data between  
10 a dealer and application providers, OEMs, and other third parties. These interfaces can be  
11 scaled and optimized to a given third party's legitimate needs to provide its service. By  
12 contrast, unauthorized third parties generally gain access to the Plaintiffs' DMSs by  
13 pretending to be dealer employees, using systems that were designed for human users.  
14 Allowing human access while blocking machine access to computer systems reflects basic  
15 computer system design and optimizes the performance, availability, confidentiality, and  
16 integrity of the system for both dealership employees and authorized third parties.

17 117. CDK's analyses have shown that hostile data extraction repeatedly and  
18 unnecessarily queries the same dealership DMS's human-user interface tens of thousands  
19 of times a day, querying *all* data in multiple files beyond what appears necessary and/or  
20 without limiting its queries to new or updated data. These human-user interfaces are not  
21 designed for the demands of automated extraction methods. Reynolds has similarly  
22 experienced automated querying at a rate of hundreds or even thousands of computing  
23 requests per day from a single data extractor. Plaintiffs' internal analyses show that these  
24 operations have taken more data than necessary to provide the service requested of the third-  
25 party extractor by the dealer.

26

1           118. The burdens on Plaintiffs' DMSs resulting from unauthorized third-party  
2 access and querying are real and measurable. For example, in some instances, third-party  
3 data extractors access more than 10 times the number of records that a vendor would access  
4 (and would need to access) to obtain a comparable dataset using CDK's managed Partner  
5 Program API. The data extractors' inefficient and poorly constructed queries can take many  
6 times longer to complete than comparable queries executed through the Partner Program  
7 interface. Similarly, since the early 2000s, third-party actions have impaired the  
8 functionality of the Reynolds DMS on many occasions. The speed and volume of automated  
9 scripts in particular taxes the computational and network resources of the Reynolds DMS,  
10 degrading services for dealers and increasing Reynolds's operational costs.

11           119. In addition to extracting data from Plaintiffs' DMSs, some unauthorized third  
12 parties also attempt to write altered data back onto the DMS. Such unauthorized, automated  
13 activity creates a high risk of introducing data errors and undermining the integrity of the  
14 DMSs. A series of errors by automated systems can rapidly propagate across an entire  
15 dataset, causing major disruption or even service denials. And because these hostile third  
16 parties do not use Plaintiffs' approved methods of DMS access, and the DMS Law prohibits  
17 Plaintiffs from placing any "technical or contractual" bounds on the access, Plaintiffs are  
18 limited in their ability to trace and correct DMS data that a vendor erroneously writes to the  
19 system. If the DMS Law goes into effect, Plaintiffs will also be subject to criminal penalties  
20 if they stop unauthorized activity.

## 21                           **2. Hostile Access Creates Security Threats**

22           120. Unauthorized third-party access to Plaintiffs' DMSs through a human-user  
23 interface is significantly less secure than the managed interfaces that Plaintiffs require third-  
24 party vendors to use.

25           121. Participants in CDK's Partner Program access a CDK DMS through pre-  
26 defined integration points, which act as intermediaries between the participants'

1 applications and the actual DMS. Before allowing any data to be transferred in or out of the  
2 DMS, the application must satisfy rigorous authentication protocols. And the authentication  
3 token that each application uses is transmitted through a secured communication channel.  
4 By contrast, most third-party data syndicators use dealer-issued login credentials that the  
5 syndicators often obtain through unsecured channels, including unencrypted, plain-text  
6 email. This exposes the credentials—and by extension, data on CDK’s DMS—to  
7 interception or compromise and violates widely accepted cybersecurity practices.

8 122. Reynolds launched its RCI program in the early 2000s and has invested  
9 heavily in it ever since. The RCI program facilitates customized interfaces allowing third  
10 parties to leverage the benefits of the DMS, while imposing constructed layers of security  
11 protections between the vendors and the DMS itself. The RCI program provides application  
12 vendors with the ability to both receive and, if appropriate, securely push data into the DMS  
13 via an interface that ensures the vendor receives and pushes only what is necessary for the  
14 dealer’s business needs for that vendor.

15 123. The RCI program’s innovative design has enabled Reynolds to scale its DMS  
16 systems to handle the intense amount of interoperability between Reynolds, OEMs,  
17 application providers, credit bureaus, and other third parties in a secure manner. Reynolds’s  
18 interface protocols ensure that third parties do not directly access the DMS and do not  
19 interfere with other critical dealer processes. Reynolds regularly implements security  
20 updates to combat any and all attempts by any unlicensed third party to access its systems—  
21 protecting the system from malicious cyber criminals and “hostile” third parties alike.

22 124. Hostile access also violates the fundamental security tenet known as data  
23 minimization or least privilege access, which—consistent with the GLBA—holds that each  
24 user of a secured system should receive no greater access or privileges than necessary.  
25 Plaintiffs’ certified third-party access programs ensure that each participant accesses only  
26 the specific categories of data needed for that party’s approved purposes. By contrast, third-

1 party data extractors access and extract data from all primary directories in the Plaintiffs’  
2 DMSs.

3 125. Finally, hostile access impedes Plaintiffs’ ability to audit and remain  
4 accountable to dealers and other third parties from whom they license data for the  
5 movement of data. Hostile third parties extract huge amounts of data from the DMS and  
6 sell or syndicate that data to third parties, who may resell or re-syndicate it further. Plaintiffs  
7 have no way of knowing where this data is going or how it will be used. By contrast, when  
8 third parties use Plaintiffs’ certified third-party access programs to interoperate with the  
9 DMS, those third parties agree to use the data only for approved purposes.

#### 10 **I. The DMS Law**

11 126. In introducing the bill for discussion before the Arizona Senate  
12 Transportation and Public Safety Committee, bill sponsor Arizona State Representative  
13 Noel Campbell incorrectly described it as a cybersecurity measure to protect consumers,  
14 explaining that in purchasing a car from a dealer, “you’re going to give up information  
15 about yourself that I’m sure that the consumer does not want released out in the ether.” But  
16 by requiring Plaintiffs to allow unrestricted access to their DMSs, that is precisely what the  
17 DMS Law will do.

##### 18 **1. The DMS Law’s Basic Features Harm Plaintiffs and Customers**

19 127. Although Arizona has not previously regulated the relationship between  
20 dealers and DMS providers, the DMS law effectively rewrites key provisions of contracts  
21 between Plaintiffs and Arizona car dealerships.

22 128. Section 28-4651 of the DMS Law defines a “dealer data vendor” to include  
23 “a dealer management system provider [or] consumer relationship management system  
24 provider.” CDK and Reynolds each meet this definition of a “dealer data vendor.” The  
25 definition of “dealer data vendor,” however, also includes any vendor providing a system  
26 “that permissibly stores protected dealer data pursuant to a contract with a dealer.” This

1 would include vendors that license customer relationship management, digital marketing,  
2 electronic vehicle registration and titling, and other software to facilitate dealership business  
3 operations, including, for example, any cloud storage company.

4 129. “Protected dealer data” is defined very broadly by the DMS Law to include  
5 nonpublic personal information about consumers and any “other data that relates to a  
6 dealer’s business operations in the dealer’s dealer data system.” It is not limited to data  
7 properly owned by the dealership.

8 130. The DMS Law defines a covered “dealer data system” to mean *any* “software,  
9 hardware, or firmware system that is owned, leased or licensed by a dealer” and that “stores  
10 or provides access to protected dealer data.” As discussed, this sweeps very broadly to  
11 include even the software used to run routers and other hardware devices. Thus, the DMS  
12 Law applies to much more than DMS providers. Because it covers *any* software, hardware,  
13 or firmware provided by a vendor that stores *any* protected dealer data, the law also applies  
14 *a fortiori* to the word processing system the dealer uses, the dealer’s CRM software, the  
15 dealer’s tax software, and the diagnostic equipment in the dealer’s service bays, among  
16 countless other examples.

17 131. Section 28-4653 of the DMS Law prohibits a DMS provider from “tak[ing]  
18 *any action* by contract, technical means or otherwise to prohibit or limit a dealer’s ability  
19 to protect, store, copy, share or use protected dealer data.” (Emphasis added.) This includes  
20 “imposing *any* fee or other restriction on the dealer or an authorized integrator for accessing  
21 or sharing protected dealer data or for writing data to a dealer data system.” (Emphasis  
22 added.) But that section also prohibits a third party from placing “*unreasonable*  
23 restriction[s] on integration.” (Emphasis added.) Dealer data vendors are thus left with an  
24 irreconcilable ambiguity over how to comply with a law that prohibits “any” restrictions  
25 but at the same time prohibits only “unreasonable” restrictions.

26



1           132. The DMS Law forbids a DMS provider from placing any restriction—  
2 including a fee—on access by “authorized integrators.” An “authorized integrator” is any  
3 third party “with whom a *dealer* enters into a contractual relationship to perform a specific  
4 function for the dealer that allows the third party to access protected dealer data or to write  
5 data to a dealer data system, or both, to carry out the specified function.” In other words,  
6 under the DMS Law, a hostile and unauthorized third-party data extractor or writer becomes  
7 an “authorized integrator” at the sole discretion of a dealer—with no input from, control by,  
8 or protection for Plaintiffs. Plaintiffs may not prohibit any third party that the dealer has  
9 identified as one of its authorized integrators from accessing and using that dealer’s dealer  
10 data system, so long as the third party complies with standards deemed acceptable by the  
11 dealer.

12           133. The DMS Law further bars Plaintiffs from placing certain restrictions “on the  
13 scope or nature of the data that is shared with an authorized integrator” or “on the ability of  
14 the authorized integrator to write data to a dealer data system.” Nor may Plaintiffs place  
15 certain “limitation[s] or condition[s] on a third party that accesses or shares protect[ed]  
16 dealer data or that writes data to a dealer data system.”

17           134. Section 28-4653 of the DMS Law states that it “does not prevent a dealer,  
18 manufacturer or third party from discharging its obligations as a service provider or  
19 otherwise under federal, state or local law to protect and secure protected dealer data,” but  
20 it would be impossible for Plaintiffs to comply with the DMS Law *without* violating several  
21 such obligations.

22           135. The DMS law works at cross purposes with federal and state data privacy  
23 laws. In late 2016, a hacker broke into a DMS called DealerBuilt because of poor security  
24 practices that created an unsecured access point into a backup database storing sensitive  
25 consumer data, including names, addresses, telephone numbers, Social Security numbers,  
26 driver’s license numbers, dates of birth, credit card information, and other data. For at least

1 ten days, the hacker had access to the records of 12.5 million consumers stored on this  
2 backup database and downloaded the personal information of nearly 70,000 consumers  
3 from the backup directories of just five dealerships.

4 136. By Consent Order with the Federal Trade Commission, DealerBuilt now must  
5 implement a detailed information security program, including implementing technical  
6 measures to monitor unauthorized attempts to extract data from its networks, data access  
7 controls for all databases storing personal information, and encrypting all Social Security  
8 numbers and financial account information. To comply with the Order, DealerBuilt must,  
9 at a minimum, restrict inbound connections to IP addresses, require authentication to access  
10 the databases, and limit employee access to what is needed to perform that employee's job  
11 function.

12 137. Additionally, pursuant to a separate consent decree with one state, the  
13 DealerBuilt DMS is required by court order to "maintain and implement reasonable access  
14 control Policies that clearly define which users have authorization to access its Computer  
15 Network, and [to] maintain reasonable enforcement mechanisms to approve or disapprove  
16 access requests based on those Policies."

17 138. By contrast, the DMS Law *prevents* DMS providers (including DealerBuilt)  
18 from taking any measures to prevent access to their systems. DMS providers cannot comply  
19 with both the security mandates imposed by federal and state law, on the one hand, and the  
20 DMS Law on the other.

21 139. Section 28-4654 of the DMS Law requires Plaintiffs to "make any agreement  
22 regarding access to, sharing or selling of, copying, using or transmitting protected dealer  
23 data terminable on ninety days' notice from the dealer."

24 140. Section 28-4654 further requires Plaintiffs to "[a]dopt and make available a  
25 standardized framework for the exchange, integration and sharing of data from dealer data  
26 systems with authorized integrators and the retrieval of data by authorized integrators."

1 Section 28-4654 requires Plaintiffs to “[p]rovide access to open application programming  
2 interfaces” or “a similar open access integration method” to authorized integrators, and  
3 requires Plaintiffs to provide “unrestricted access to all protected dealer data and all other  
4 data stored in the dealer data system” upon a dealer’s notice of intent to terminate an  
5 agreement with a dealer data vendor.

6 141. Section 28-4654 also requires Plaintiffs to provide “access to or an electronic  
7 copy of all protected dealer data and all other data stored in the dealer data system in a  
8 commercially reasonable time and format that a successor dealer data vendor or authorized  
9 integrator can access and use” upon notice of the dealer’s intent to terminate its contract.  
10 And the same section requires Plaintiffs to “allow a dealer to audit the dealer data vendor  
11 or authorized integrator’s access to and use of any protected dealer data.”

12 142. In effectively requiring Plaintiffs to grant access to their DMSs, routers, and  
13 other hardware devices to any third party at the dealers’ sole discretion, Sections 28-4653  
14 and 28-4654 compel Plaintiffs to exchange data, intellectual property, and other information  
15 with third parties. The DMS Law mandates open access to the sensitive categories of  
16 information that flow through Plaintiffs’ systems while simultaneously prohibiting  
17 Plaintiffs from taking measures to protect that information as required by federal and state  
18 data protection and privacy laws. Moreover, complying with these sections, if possible at  
19 all, would require Plaintiffs to draft computer code to change the basic functionality of parts  
20 of their DMSs, and would thereby compel Plaintiffs to engage in protected speech.

21 143. These provisions retroactively rewrite Plaintiffs’ negotiated contracts and  
22 undercut Plaintiffs’ extensive efforts to protect the confidentiality, integrity, and availability  
23 of their DMSs by limiting access to authorized users and barring or detecting unauthorized  
24 intrusions. These provisions encroach on Plaintiffs’ property rights by preventing Plaintiffs  
25 from excluding others from their systems; moreover, they do so for the benefit of private  
26 parties rather than for public purposes. And, in so doing, these provisions even require

1 Plaintiffs to permit third parties to write data to Plaintiffs' systems and hardware,  
2 notwithstanding the serious risks associated with that practice.

3 144. These provisions permit third parties to use, copy, and distribute Plaintiffs'  
4 original copyrighted material without compensation, while simultaneously barring  
5 Plaintiffs from implementing contractual and/or technical measures to protect their  
6 exclusive rights as copyright owners.

## 7 **2. The DMS Law is Hopelessly Vague**

8 145. Numerous provisions of the DMS Law are so vague that they fail to place  
9 Plaintiffs on notice of what conduct is permitted and what conduct might subject them to  
10 criminal penalties under the law, including the provisions discussed below.

11 146. Section 28-4652 prohibits Plaintiffs (as "third parties") from "requiring" a  
12 dealer to grant Plaintiffs or their agents direct or indirect access to the dealer's data system.  
13 But Plaintiffs do not "require" dealers to do anything; they enter into voluntary contracts  
14 with dealers desiring access to their services. And by virtue of owning and operating their  
15 DMSs, Plaintiffs necessarily have employees or agents that have access to the computer  
16 systems to develop, monitor, and operate these systems. This provision fails to inform  
17 Plaintiffs whether conditions in those voluntary agreements constitute unlawful  
18 "requirements" and whether the fact that Plaintiffs' employees or agents have access to their  
19 own proprietary systems violates the law.

20 147. Section 28-4653.A.2 prohibits Plaintiffs (as "third parties") from engaging in  
21 any act of "cyber ransom," which means "to encrypt, restrict or prohibit or threaten or  
22 attempt to encrypt, restrict or prohibit a dealer's or a dealer's authorized integrator's access  
23 to protected dealer data for monetary gain." As with Section 28-4652, this provision does  
24 not inform Plaintiffs whether it is a violation to *agree with* dealers to host and encrypt their  
25 data for a fee. If this is not a violation, then this provision also fails to inform Plaintiffs

26

1 whether it is “cyber ransom” for them to restrict access to paying dealers’ data by non-  
2 paying dealers or third parties.

3 148. Section 28-4653.A.3 prohibits Plaintiffs (as “third parties”) from taking “any  
4 action by contract, technical means or otherwise to prohibit or limit a dealer’s ability to  
5 protect, store, copy, share or use protected dealer data.” This provision does not make clear  
6 whether it is limited to *that dealer’s* protected dealer data or *all* protected dealer data. That  
7 is, it does not place Plaintiffs on notice of whether it is a criminal violation for them to limit  
8 one dealer’s ability to copy or use protected dealer data belonging to another dealer.

9 149. Section 28-4653.A.3(a) prohibits Plaintiffs (as “third parties”) from imposing  
10 any “fee” on a dealer or authorized integrator for access to protected dealer data. “Fee” is  
11 defined as a charge “beyond any direct costs incurred” by Plaintiffs (as “dealer data  
12 vendors”) in providing such access “to an authorized integrator or allowing an authorized  
13 integrator to write data to a dealer data system.” *Id.* § 28-4651.5. This is impermissibly  
14 vague on two levels.

15 150. First, “fee” is defined with reference to Plaintiffs’ costs to provide access to  
16 authorized integrators, with no reference to their costs to provide access to dealers. But  
17 Section 28-4653.A.3(a) prohibits charging fees for access by dealers. This may mean  
18 Plaintiffs cannot charge *anything* to dealers (because, by definition, this would be a charge  
19 beyond any direct costs incurred by Plaintiffs in providing access to authorized integrators),  
20 or it may mean that only charges to authorized integrators can be classified as impermissible  
21 fees. The law fails to inform Plaintiffs which of these two constructions is correct, and thus  
22 which charges will trigger a violation.

23 151. Second, “direct” costs are not defined. Considering all of the costs required  
24 for Plaintiffs merely to maintain systems capable of interfacing with authorized integrators,  
25 there is no way for Plaintiffs to know where to draw the line between “direct” costs (which  
26 may be charged) and any higher charge (which constitutes a criminal fee). When accused

1 of drawing the line in the wrong place, Plaintiffs will be at the mercy of a judge's or jury's  
2 subjective interpretation of how direct is "direct."

3 152. Section 28-4653.A.3(b) prohibits Plaintiffs (as "third parties") from placing  
4 certain "unreasonable restrictions" on dealer data system access by authorized integrators.  
5 "Unreasonable" is not defined except by a non-exhaustive list of five examples, four of  
6 which incorporate the undefined term "unreasonable." Without more, Plaintiffs cannot  
7 begin to determine which restrictions are prohibited, especially considering that Section 28-  
8 4653.A.3 prohibits "*any* action" to limit a dealer's ability to share or use protected dealer  
9 data.

10 153. Another example of the vague language permeating the DMS Law is Section  
11 28-4655, which provides that the DMS Law does not "govern, restrict or apply to data that  
12 exists outside of a dealer data system, including data that is generated by a motor vehicle."  
13 A key component of "protected dealer data," however, is "motor vehicle diagnostic data  
14 that is stored in a dealer data system." *See* § 28-4651.7(b). This is vague in at least three  
15 respects.

16 154. First, once external motor vehicle data is transmitted to a dealer data system,  
17 it is unclear whether it (a) becomes protected dealer data, taking it outside the exclusion of  
18 Section 28-4655 and making it subject to the DMS Law, or (b) remains subject to the  
19 exclusion (and thus *not* subject to the DMS Law) as long as it still exists outside the dealer  
20 data system. That is, it is unclear whether "exists outside of a dealer data system" means  
21 "exists *solely* outside of a dealer system," or "*also* exists outside of whatever dealer data  
22 system it may be in."

23 155. Second, if the latter is the correct interpretation, then it is also unclear whether  
24 Section 28-4655 applies to (i.e., exempts) that data wherever it is stored (including within  
25 a dealer data system), or only whatever copies of the data exist outside the dealer data  
26 system.

1           156. Third, regardless of which of these interpretations is correct, there is no way  
2 for Plaintiffs—regulated parties subject to criminal penalties for non-compliance—to know  
3 whether data entered into their DMS also exists outside of it.

4           157. Even setting aside all of these deficiencies, the application of the *entire DMS*  
5 *Law* to Plaintiffs' conduct is vague due to Section 28-4653.C, which provides that the law  
6 does not prevent third parties (including Plaintiffs) from discharging their obligations, as  
7 service providers or otherwise, under federal, state or local law to protect and secure  
8 protected dealer data. But the entire purpose of the DMS Law is to prohibit Plaintiffs from  
9 implementing the technological and operational measures that Plaintiffs have developed  
10 based on their understanding of their legal obligations to protect and secure protected dealer  
11 data.

12           158. It is therefore impossible for Plaintiffs to comply with these obligations and  
13 the conflicting provisions of the DMS Law. But the DMS Law itself provides no clear  
14 guidance as to which of these will control. That is, it is ultimately unclear whether the DMS  
15 Law applies to Plaintiffs *at all*.

#### 16                   **J. The Current Controversy**

17           159. On April 9, 2019, Governor Ducey signed House Bill 2418 into law. The  
18 DMS Law will become effective 90 days after the close of the regular session of the Fifty-  
19 Fourth Legislature, or on August 26, 2019.

20           160. Because the DMS Law will become effective in just a few weeks, Plaintiffs  
21 face imminent enforcement of the DMS Law against them by Defendants.

22           161. Additionally, the new statutory obligations imposed upon Plaintiffs regarding  
23 third-party access to their DMSs pose a real and immediate threat to Plaintiffs' property and  
24 contract rights and to the security of the DMSs.

25  
26



1 **FIRST CLAIM FOR RELIEF**

2 **Declaratory Judgment**

3 **(Conflict Preemption, Digital Millennium Copyright Act)**

4 162. Paragraphs 1–161 above are incorporated herein by reference.

5 163. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
6 Court’s inherent equitable authority, and seeks a declaration that the DMS Law is  
7 unenforceable because it is preempted by the federal Digital Millennium Copyright Act.

8 164. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI,  
9 provides that “the laws of the United States . . . shall be the supreme law of the land.”

10 165. State laws that conflict with federal law are preempted by operation of the  
11 Supremacy Clause.

12 166. Preemption may arise in a variety of contexts, including when the state law  
13 conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal  
14 law.

15 167. Congress enacted the DMCA, 17 U.S.C. § 1201, to reinforce copyright  
16 owners’ rights to use technological defenses to control access to and prevent the copying of  
17 copyrighted material. The DMCA establishes penalties for those who circumvent copyright  
18 owners’ technological defenses and prohibits commerce in products or services designed to  
19 facilitate circumvention of copyright owners’ technological defenses. Section  
20 1201(a)(1)(A) of the DMCA provides that no “person shall circumvent a technological  
21 measure that effectively controls access to a work protected under this title.” Section  
22 1201(a)(2) reinforces that prohibition by banning commerce in products and services  
23 intended to facilitate circumvention of access controls.

24 168. The DMCA is not only enforceable criminally, *id.* § 1204, but also offers  
25 copyright owners a private right of action against those who unlawfully access an owner’s  
26 work, *id.* § 1203.

1           169. CDK's DMS software is an original creative work protected under Title 17.  
2 Among its original and creative elements are its source and object code; distinctive screen  
3 layouts; graphical content; text; arrangement, organization, and display of information; and  
4 dynamic user experience.

5           170. The Reynolds DMS PC software program is an original creative work  
6 protected under Title 17. Among the many significant original elements of the program are  
7 its source and object code; distinctive screen layouts; graphical content; text; arrangement,  
8 organization, and display of information; and dynamic user experience. Reynolds has  
9 registered copyrights on multiple versions of the Reynolds DMS software program.  
10 (Registration Nos. TX 7-586-896; TX 7-586-863; TX 8-538-825; and TX 8-538-541). The  
11 application software on the dealer PC and on the DMS server that is accessed by the DMS  
12 PC software program is also original creative work protected under Title 17. Among the  
13 many significant original elements of these programs are their source and object code;  
14 distinctive page layouts; graphical content; text; arrangement, organization, and display of  
15 information; and dynamic user experience.

16           171. CDK uses several technological measures to control access to and prevent  
17 copying of the CDK DMS software program. These technological measures include:  
18 requiring CDK dealer employees to log on with passwords; text prompts asking a user to  
19 certify that the user is an authorized dealer employee; CAPTCHA controls; and disabling  
20 dealer credentials that CDK finds have been used for automated access by third parties.  
21 These measures effectively control access to the DMS software program because the  
22 program, or portions of it, cannot be run, and its original, expressive elements cannot be  
23 displayed or copied, unless these measures have been navigated.

24           172. Reynolds deploys numerous technological measures that effectively control  
25 access to and copying of the Reynolds DMS software or portions thereof. These  
26 technological access-control measures include login prompts that require a user to enter a

1 valid username and password to access the system; CAPTCHA controls that require a user  
2 to successfully solve a CAPTCHA to access certain portions of the Reynolds DMS software  
3 (including the Reynolds DMS data exporting functions); and Reynolds's Suspicious User  
4 ID monitoring software (which identifies login credentials that use automated scripts and  
5 bots and flags those credentials for deactivation). In the ordinary course of their operation,  
6 these technological measures require application of information, or a process or treatment,  
7 with Reynolds's authority as the owner of the DMS, to gain access to the Reynolds DMS  
8 software. These measures effectively control access to the DMS software program because  
9 the program, or portions of it, cannot be run, and its original, expressive elements cannot be  
10 accessed, displayed, or copied, unless these measures have been navigated.

11 173. The DMCA prohibits hostile third parties from circumventing these  
12 technological measures without CDK's or Reynolds's authorization, and gives CDK and  
13 Reynolds an enforceable right against such circumvention. Moreover, the statute prohibits  
14 hostile third parties from offering services that facilitate circumvention of the above-  
15 described technological measures. CDK and Reynolds, in turn, have an enforceable right to  
16 erect technological measures against hostile third parties' unauthorized access to and  
17 copying of their respective copyrighted DMS software.

18 174. The DMS Law stands as an obstacle to the purposes behind, and is preempted  
19 by, the DMCA because it effectively compels CDK and Reynolds to abandon the  
20 technological measures that they have adopted to control access to their copyrighted works  
21 and that Congress has authorized them to employ. Contrary to the DMCA, copyright owners  
22 must jettison these technological measures and grant access to any third party designated  
23 by a dealer without a license or authorization from the DMS provider.

24 175. Thus, the DMS Law conflicts with the DMCA and is preempted.  
25  
26

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

**SECOND CLAIM FOR RELIEF**  
**Declaratory Judgment**  
**(Conflict Preemption, Copyright Act)**

176. Paragraphs 1–175 above are incorporated herein by reference.

177. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court’s inherent equitable authority, and seeks a declaration that the DMS Law is unenforceable because it is preempted by the federal Copyright Act.

178. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that “the laws of the United States . . . shall be the supreme law of the land.”

179. State laws that conflict with federal law are preempted by operation of the Supremacy Clause.

180. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

181. The Copyright Act, 17 U.S.C. § 101, *et seq.*, offers protection to creators of copyrightable material, including the right to exclude others from copying, distribution, preparation of derivative works based on, and displaying copyrighted works.

182. As explained, Plaintiffs’ DMSs contain and are comprised of copyrighted and copyrightable material.

183. The DMS Law conflicts with, and is preempted by, the federal Copyright Act because it eliminates the copyright owner’s right to exclude others from copying, distributing, creating derivative works based on, or displaying the copyrighted or copyrightable material by requiring the owner to allow third parties with no license agreement with Plaintiffs to access and use Plaintiffs’ copyrighted DMS software. Such access and use necessarily entails the display, distribution, and creation of copies and derivative works of the copyrighted DMS software. As explained above, each time a user

1 runs the DMS software, that process creates a new fixed copy of the original computer  
2 program code in the computer's random access memory; new fixed copies of the program's  
3 original graphical content, text, screen layouts, and dynamic user experience; and displays  
4 those original copyrighted features on the computer screen. Moreover, allowing third parties  
5 to remotely access the DMS entails distribution of new copies of the software.

6 184. Thus, the DMS Law conflicts with the Copyright Act and is preempted.

7 **THIRD CLAIM FOR RELIEF**

8 **Declaratory Judgment**

9 **(Conflict Preemption, Defend Trade Secrets Act)**

10 185. Paragraphs 1–184 above are incorporated herein by reference.

11 186. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
12 Court's inherent equitable authority, and seeks a declaration that the DMS Law is  
13 unenforceable because it is preempted by the federal Defend Trade Secrets Act ("DTSA").

14 187. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI,  
15 provides that "the laws of the United States . . . shall be the supreme law of the land."

16 188. State laws that conflict with federal law are preempted by operation of the  
17 Supremacy Clause.

18 189. Preemption may arise in a variety of contexts, including when the state law  
19 conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal  
20 law.

21 190. The DTSA, 18 U.S.C. § 1836, *et seq.*, protects owners of trade secrets from  
22 misappropriation by third parties. Meant by Congress as a powerful tool for the protection  
23 of trade secrets, the Act not only establishes criminal penalties, but also gives the owner of  
24 a trade secret that is misappropriated a private right of action against anyone who discloses  
25 or uses that secret without the owner's consent despite knowing or having reason to know  
26

1 that knowledge of the trade secret was derived from or through someone who had a duty to  
2 maintain the owner's secret.

3 191. CDK's DMS contains numerous CDK-proprietary trade secrets, including  
4 CDK-related forms, accounting rules, tax tables, and proprietary tools and data  
5 compilations. These trade secrets relate to CDK's DMS services, which are licensed and/or  
6 sold in interstate and foreign commerce. As described in greater detail above, CDK has  
7 taken reasonable measures to keep its trade secrets secret.

8 192. Reynolds's DMS contains numerous Reynolds-proprietary trade secrets,  
9 including Reynolds-related forms, accounting rules, tax tables, and proprietary tools and  
10 data compilations. These trade secrets relate to Reynolds's DMS services, which are  
11 licensed and/or sold in interstate and foreign commerce. As described in greater detail  
12 above, Reynolds has taken reasonable measures to keep its trade secrets secret. State laws  
13 that conflict with federal law are preempted by operation of the Supremacy Clause.

14 193. The DMS Law conflicts with, and is preempted by, the Defend Trade Secrets  
15 Act because it deprives Plaintiffs of their federally protected rights to exclude others from  
16 their trade secrets by requiring CDK and Reynolds to provide access to third parties  
17 authorized by the dealers, not by CDK or Reynolds.

18 194. Thus, the DMS Law conflicts with the DTSA and is preempted.

19 **FOURTH CLAIM FOR RELIEF**

20 **Declaratory Judgment**

21 **(Conflict Preemption, Computer Fraud and Abuse Act)**

22 195. Paragraphs 1–194 above are incorporated herein by reference.

23 196. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
24 Court's inherent equitable authority, and seeks a declaration that the DMS Law is  
25 unenforceable because it is preempted by the federal Computer Fraud and Abuse Act.  
26

1           201. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI,  
2 provides that “the laws of the United States . . . shall be the supreme law of the land.”

3           202. State laws that conflict with federal law are preempted by operation of the  
4 Supremacy Clause.

5           203. Preemption may arise in a variety of contexts, including when the state law  
6 conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal  
7 law.

8           204. The CFAA provides that “[w]hoever . . . intentionally accesses a computer  
9 without authorization or exceeds authorized access, and thereby obtains . . . information  
10 from any protected computer,” is subject to criminal and civil liability. 18 U.S.C.  
11 § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages  
12 and injunctive relief).

13           205. In enacting the CFAA, Congress intended to empower businesses and  
14 individuals to control who may access their computer systems by prohibiting hackers and  
15 others from accessing computers without the owners’ authorization. Under the statute,  
16 computer owners have exclusive discretion to decide who is authorized to access their  
17 computer and for what purposes.

18           206. To effectuate these aims, the CFAA is not only enforceable criminally, but  
19 also permits any private person “who suffers damages or loss by reason of a violation of”  
20 the statute to “maintain a civil action against the violator to obtain compensatory damages  
21 and injunctive relief or other equitable relief,” *id.* § 1030(g).

22           207. A DMS is a “computer” within the meaning of the CFAA, which defines that  
23 term to include “any data storage facility or communications facility directly related to or  
24 operating in conjunction with [a computing] device.” *Id.* § 1030(e)(1). Plaintiffs’ DMSs  
25 also rely on the operation of one or more computing devices in their operations. The DMSs  
26 themselves, and the computing devices by which they operate, are “protected computers”



1 within the statute’s meaning because they are connected to the internet and thus are used in  
2 and affect interstate and foreign commerce and communications. *See id.* § 1030(e)(2)(B).

3 204. Contrary to Congress’s purpose in enacting the CFAA, Arizona’s DMS Law  
4 removes Plaintiffs’ rights to determine who is an authorized user of their DMSs, or for what  
5 purpose third parties may use their DMSs, by requiring CDK and Reynolds to allow access  
6 to their systems by any user authorized by a *dealer*, even if not authorized by CDK or  
7 Reynolds.

8 205. Thus, the DMS Law conflicts with the CFAA and is preempted.

9 **FIFTH CLAIM FOR RELIEF**

10 **Declaratory Judgment**

11 **(Conflict Preemption, Gramm-Leach-Bliley Act)**

12 206. Paragraphs 1–205 above are incorporated herein by reference.

13 207. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
14 Court’s inherent equitable authority, and seeks a declaration that the DMS Law is  
15 unenforceable because it is preempted by the GLBA.

16 208. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI,  
17 provides that “the laws of the United States . . . shall be the supreme law of the land.”

18 209. State laws that conflict with federal law are preempted by operation of the  
19 Supremacy Clause.

20 210. Preemption may arise in a variety of contexts, including when the state law  
21 conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal  
22 law.

23 211. The GLBA provides “that each financial institution has an affirmative and  
24 continuing obligation to respect the privacy of its customers and to protect the security and  
25 confidentiality of those customers’ nonpublic personal information.” 15 U.S.C. § 6801(a).  
26 In furtherance of this law, the Federal Trade Commission’s Safeguards Rule requires

1 financial institutions such as automobile dealerships to employ administrative, technical,  
2 and physical safeguards to protect sensitive customer information at issue. *See* 16 CFR Part  
3 314.3.

4 212. In addition to implementing their own safeguards, financial institutions such  
5 as dealerships must take steps to ensure that their service providers—such as Plaintiffs and  
6 other DMS providers—similarly safeguard customer information in their care. *Id.*  
7 § 314.4(d).

8 213. The DMS Law forbids Plaintiffs from taking any measures to secure their  
9 systems or limit the data that a third party can access, extract, or modify on the DMS.

10 214. The DMS Law further bars Plaintiffs from placing certain restrictions “on the  
11 scope or nature of the data that is shared with an authorized integrator” or “on the ability of  
12 the authorized integrator to write data to a dealer data system.” Nor may Plaintiffs place  
13 certain “limitation[s] or condition[s] on a third party that accesses or shares protect[ed]  
14 dealer data or that writes data to a dealer data system.”

15 215. Contrary to Congress’ intent, the DMS Law requires DMS providers to create  
16 a gaping vulnerability in DMSs that impacts thousands of dealer licensees and hundreds of  
17 millions of consumers within and without Arizona’s borders.

18 216. Such provisions directly conflict with, and are preempted by, the GLBA’s  
19 requirements that financial institutions and their service providers use technical measures  
20 to secure and protect consumer data. The DMS Law also poses an obstacle to the purposes  
21 sought to be achieved by the federal law and undermines federal policy as embodied in the  
22 GLBA and related regulations.

23 217. Thus, the DMS Law conflicts with the GLBA and is preempted.  
24  
25  
26

1 **SIXTH CLAIM FOR RELIEF**

2 **Declaratory Judgment**

3 **(Void for Vagueness, United States Constitution)**

4 218. Paragraphs 1–217 above are incorporated herein by reference.

5 219. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
6 Court’s inherent equitable authority, and seeks a declaration that the DMS Law is  
7 unenforceable because it is void for vagueness under the U.S. Constitution.

8 220. The Constitution provides that no State shall deprive any person of property  
9 without due process of law. U.S. Const. amend. XIV.

10 221. It is a basic principle of due process that a law is void for vagueness if its  
11 prohibitions are not clearly defined—that is, if it fails to give a person of ordinary  
12 intelligence a reasonable opportunity to know what is prohibited.

13 222. Laws imposing criminal sanctions, as the DMS Law does, are subject to a  
14 more demanding standard of scrutiny when challenged for vagueness.

15 223. As the foregoing, non-exhaustive list demonstrates (*infra* ¶ 224(a)-(g),  
16 numerous aspects of the DMS Law would deprive Plaintiffs of property without a  
17 reasonable opportunity to know what is prohibited or required.

18 224. Indeed, the DMS Law is riddled with ambiguities going to the heart of nearly  
19 every operative provision affecting Plaintiffs, who cannot know:

- 20 (a) Whether contractually agreed dealer access restrictions violate the law;  
21 (b) Whether hosting encrypted data for a fee is prohibited cyber-ransom;  
22 (c) Whether they are required to facilitate or prevent one dealer from accessing  
23 another dealer’s data;  
24 (d) Whether any or all of their dealer charges are prohibited fees;  
25 (e) Which of their restrictions on access by authorized integrators are  
26 “unreasonable”;

1 (f) What subset of dealer data is actually subject to the law; or even

2 (g) Whether, in light of conflicting federal obligations, the law applies to  
3 Plaintiffs or their core conduct *at all*.

4 225. In light of these fundamental ambiguities, which are not severable from the  
5 DMS Law as a whole, the Act is unconstitutionally vague on its face and as applied to  
6 Plaintiffs—particularly under the heightened scrutiny triggered by criminal liability.

7 **SEVENTH CLAIM FOR RELIEF**

8 **Declaratory Judgment**

9 **(Unconstitutional Taking, United States Constitution)**

10 226. Paragraphs 1–225 above are incorporated herein by reference.

11 227. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
12 Court’s inherent equitable authority, and seeks a declaration that the DMS Law is  
13 unenforceable because it works an unconstitutional taking under the U.S. Constitution.

14 228. The Constitution provides that private property may not be taken for public  
15 use without just compensation. U.S. Const. amend. V.

16 229. The DMS Law takes Plaintiffs’ private property by requiring CDK and  
17 Reynolds to allow third parties to access their proprietary DMSs and to remove data and  
18 write data to that system. The DMS Law takes Plaintiffs’ control over their proprietary  
19 systems and gives it to third parties. And it allows third parties to physically occupy and  
20 take part of the proprietary DMSs by allowing them to write data into that system.

21 230. The DMS Law takes private property for no public purpose but rather for the  
22 sole economic benefit of a small number of private parties—including car dealers located  
23 in Arizona and third-party data syndicators.

24 231. CDK and Reynolds spent years and millions of dollars developing their  
25 DMSs, including security measures to control access to the system, and during that time the  
26 government did not regulate the right of dealers to grant third parties access to DMSs.



1 way to advance a significant and legitimate public purpose. In fact, the law advances no  
2 public purpose but rather alters existing contractual relationships for the benefit of a small  
3 class of private parties.

## 4 **NINTH CLAIM FOR RELIEF**

### 5 **Declaratory Judgment**

#### 6 **(Violation of Dormant Commerce Clause)**

7 241. Paragraphs 1–240 above are incorporated herein by reference.

8 242. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
9 Court’s inherent equitable authority, and seeks a declaration that the DMS Law is  
10 unenforceable because it violates the dormant Commerce Clause of the U.S. Constitution.

11 243. The dormant Commerce Clause provides that any state law affecting  
12 interstate commerce may not impose an undue burden on that commerce. *See* U.S. Const.  
13 art. I, § 8, cl. 3.

14 244. The DMS Law affects interstate commerce because it regulates the  
15 relationship between DMS providers and car dealers, which conduct business across state  
16 lines in interstate commerce.

17 245. The DMS Law imposes an undue and substantial burden on interstate  
18 commerce because it creates special rules for the relationship between DMS providers and  
19 dealers. DMSs are sold nationwide, and indeed some dealers have operations in more than  
20 one State, but Plaintiffs must change their products specifically for the Arizona market as a  
21 result of the DMS Law.

22 246. Further, the DMS Law places a great quantity of private consumer  
23 information and proprietary OEM data at risk in states outside Arizona by permitting access  
24 to DMSs by users who have not been properly screened and trained by DMS providers and  
25 by dismantling the carefully designed safeguards currently in place to prevent the  
26 deleterious effects of unfettered DMS access.





1           254. The disclosure requirements imposed by the DMS Law are unjustified and  
2 unduly burdensome because they would require Plaintiffs to engage in protected speech by  
3 (i) drafting computer code to allow third parties to circumvent the security measures that  
4 currently control access to Plaintiffs’ DMSs and otherwise rewrite the functionality of the  
5 DMSs; and (ii) forcing the exchange of information with third parties, all at substantial cost  
6 and in violation of Plaintiffs’ rights.

7   **ELEVENTH CLAIM FOR RELIEF**

8   **Preliminary and Permanent Injunction**

9           255. Paragraphs 1–254 above are incorporated herein by reference.

10           256. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this  
11 Court’s inherent equitable authority.

12           257. Plaintiffs have a substantial likelihood of success on the merits of their claims.

13           258. Plaintiffs would suffer irreparable harm in the absence of an interlocutory and  
14 permanent injunction because the access to the DMSs required by the DMS Law may  
15 compromise the integrity of those systems, damaging their continued operation and placing  
16 protected consumer, OEM, third-party, and Plaintiff data at risk, while permanently and  
17 immeasurably damaging DMS providers’ reputations as sources of secure systems. The  
18 DMS Law requires Plaintiffs to allow parties authorized by dealers to write data onto the  
19 system, regardless of whether that party has been vetted by Plaintiffs. This poses the real  
20 possibility of data corruption or adding malware to the system. Additionally, Plaintiffs have  
21 taken strong measures to prevent hackers from accessing their DMSs, but the methods they  
22 have employed are undone by the DMS Law, which strips Plaintiffs of the ability to prevent  
23 access that they have not authorized. All the while, confidential information, including a  
24 vast amount of consumer information, is needlessly placed at risk by the law.

25  
26



1 H. Declaring that the DMS Law is unenforceable because it violates the  
2 Contracts Clause of the United States Constitution;

3 I. Declaring that the DMS Law is unenforceable because it violates the  
4 Dormant Commerce Clause of the United States Constitution;

5 J. Declaring that the DMS Law is unenforceable because it violates the First  
6 Amendment of the United States Constitution;

7 K. Temporarily and permanently enjoining the enforcement of the DMS Law;

8 L. Awarding Plaintiffs their costs and litigation expenses, including attorney’s  
9 fees and costs; and

10 M. Awarding Plaintiffs such other and further relief that this Court deems just,  
11 proper, and equitable.

12 RESPECTFULLY SUBMITTED this 29th day of July, 2019.

13 QUARLES & BRADY LLP  
14 Renaissance One  
15 Two North Central Avenue  
16 Phoenix, AZ 85004-2391

17 By /s/ Brian A. Howie

Brian A. Howie  
Lauren Elliott Stine

18 *Attorneys for Plaintiffs*

19 SHEPPARD, MULLIN, RICHTER &  
20 HAMPTON LLP  
21 2099 Pennsylvania Ave., NW, Ste. 100  
22 Washington, DC 20006, 201-747-1900  
23 Thomas J. Dillickrath\* (DC 483710)  
24 [TDillickrath@sheppardmullin.com](mailto:TDillickrath@sheppardmullin.com)

25 Four Embarcadero Center, 17th Floor  
26 San Francisco, CA 94111, 415-434-9100  
Amar S. Naik\* (CA 307208)  
[ANaik@sheppardmullin.com](mailto:ANaik@sheppardmullin.com)  
Molly C. Lorenzi\* (CA 315147)  
[MLorenzi@sheppardmullin.com](mailto:MLorenzi@sheppardmullin.com)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

GIBBS & BRUNS LLP  
1100 Louisiana, Ste. 5300  
Houston, TX 77002, 713-650-8805  
Aundrea K. Gulley\* (TX 24034468)  
[agulley@gibbsbruns.com](mailto:agulley@gibbsbruns.com)  
Denise Drake\* (TX 24092358)  
[DDrake@gibbsbruns.com](mailto:DDrake@gibbsbruns.com)

*Attorneys for The Reynolds and Reynolds  
Company*

MAYER BROWN LLP  
71 S. Wacker Drive  
Chicago, IL 60606  
312-782-0600  
Britt M. Miller\* (IL 6256398)  
[BMiller@mayerbrown.com](mailto:BMiller@mayerbrown.com)  
Michael A. Scodro\* (IL 6243845)  
[MScodro@mayerbrown.com](mailto:MScodro@mayerbrown.com)  
Brett E. Legner\* (IL 6256268)  
[BLegner@mayerbrown.com](mailto:BLegner@mayerbrown.com)

1999 K Street, NW  
Washington, DC 20006  
202-263-3000  
Mark W. Ryan\* (DC 359098)  
[mryan@mayerbrown.com](mailto:mryan@mayerbrown.com)

*Attorneys for CDK Global, LLC*

*\*Pro Hac Vice Forthcoming*