No. 20-16469

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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

Plaintiffs-Appellants,

vs.

Mark Brnovich, Attorney General of the State of Arizona, et al.

Defendants-Appellees.

On Appeal from the United States District Court
for the District of Arizona, No. 2:19-cv-04849-GMS
The Hon. G. Murray Snow

PLAINTIFFS-APPELLANTS' OPENING BRIEF

Brian A. Howie
Lauren E. Stine
QUARLES & BRADY LLP
Two N. Central Ave.
Phoenix, AZ 85004
Attorneys for Appellants

Britt M. Miller
Michael A. Scodro
Brett E. Legner
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606

Mark W. Ryan
1999 K Street, NW
Washington, DC 20006
Attorneys for Appellant
CDK Global, LLC

Thomas J. Dillickrath
Jonathan R. DeFosse
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
2099 Pennsylvania Ave., NW, Ste. 100
Washington, DC 20006

Molly C. Lorenzi
Four Embarcadero Center, 17th Floor
San Francisco, CA 94111

Aundrea K. Gulley
Brice A. Wilkinson
Denise Drake
GIBBS & BRUNS LLP
1100 Louisiana, Ste. 5300
Houston, TX 77002
Attorneys for Appellant
The Reynolds and Reynolds Company

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Appellants CDK Global, LLC and The Reynolds and Reynolds Company hereby submit this corporate disclosure statement.

CDK Global, LLC's ultimate parent corporation is CDK Global, Inc, which is publicly traded. No other publicly traded corporation owns 10% or more of CDK's stock.

The Reynolds and Reynolds Company's parent corporation is Dealer Computer Services, Inc.

RESPECTFULLY submitted this 27th day of August, 2020.

QUARLES & BRADY LLP
Two North Central Ave.
Phoenix, AZ 85004-2391

By:*/s/ Brian A. Howie*
Brian A. Howie
Lauren Elliott Stine

Attorneys for Appellants

Thomas J. Dillickrath
Jonathan R. DeFosse
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
2099 Pennsylvania Ave., N.W.
Suite 100
Washington, D.C. 20006

Molly C. Lorenzi
Four Embarcadero Center, 17th Fl.
San Francisco, CA 94111

Aundrea K. Gulley
Brice A. Wilkinson
Denise Drake
GIBBS & BRUNNS LLP
1100 Louisiana, Suite 5300
Houston, TX 77002
Attorneys for Appellant
The Reynolds and Reynolds Company

Britt M. Miller
Michael A. Scodro
Brett E. Legner
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606

Mark W. Ryan
1999 K St., N.W.
Washington, D.C. 20006
Attorneys for Appellant
CDK Global, LLC

TABLE OF CONTENTS

PAGE

TABLES OF AUTHORITIES iv
STATEMENT REGARDING ORAL ARGUMENT xi
JURISDICTIONAL STATEMENT 1
STATEMENT OF THE ISSUES PRESENTED 2
STATEMENT REGARDING STATUTORY ADDENDUM 3
STATEMENT OF THE CASE 3
A. THE DEALER MANAGEMENT SYSTEM 3
B. THE LAW 7
C. THE IMPACT OF COMPLIANCE WITH THE LAW ON DMS PROVIDERS 9
D. PROCEDURAL BACKGROUND OF THE CASE 11
STANDARD OF REVIEW 12
SUMMARY OF THE ARGUMENT 12
ARGUMENT 14
I. THE LAW IS PREEMPTED 14
A. THE LAW CONFLICTS WITH THE COPYRIGHT ACT 15
1. THE LAW VITIATES PLAINTIFFS' EXCLUSIVE RIGHTS IN THEIR COPYRIGHTED DMS SOFTWARE 15
2. THE LAW VITIATES PLAINTIFFS' EXCLUSIVE RIGHTS IN APIS THEY AUTHOR 19
3. THE LAW VITIATES PLAINTIFFS' EXCLUSIVE RIGHTS IN THEIR DATA COMPILATIONS 21
B. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' CFAA PREEMPTION CLAIM 23

TABLE OF CONTENTS
(CONTINUED)

PAGE

1. THE CFAA VITIATES PLAINTIFFS' RIGHT TO DETERMINE WHO IS AUTHORIZED TO ACCESS THEIR COMPUTER SYSTEMS 24

2. THE DISTRICT COURT ERRED IN READING THE CFAA "NARROWLY." 26

II. THE LAW VIOLATES THE CONTRACTS CLAUSE 27

A. THE LAW SUBSTANTIALLY IMPAIRS PLAINTIFFS' CONTRACTS 28

1. THE LAW UNDERMINES PLAINTIFFS' CONTRACTUAL BARGAINS 29

2. THE LAW INTERFERES WITH PLAINTIFFS' REASONABLE EXPECTATIONS 34

3. PLAINTIFFS CANNOT REINSTATE THEIR RIGHTS REVOKED BY THE LAW 34

B. THIS SUBSTANTIAL IMPAIRMENT IS NOT JUSTIFIED BY A LAW ENACTED ONLY TO BENEFIT A FAVORED GROUP OF COMMERCIAL ACTORS 35

1. THE LAW DOES NOT SEEK TO REMEDY A BROAD AND GENERAL SOCIAL OR ECONOMIC PROBLEM 35

2. EVEN IF THERE WERE A PUBLIC PURPOSE, THE LAW WOULD BE UNREASONABLE 39

III. THE LAW CONFLICTS WITH THE TAKINGS CLAUSE.....40

A. THE LAW IS A PER SE TAKING OF PLAINTIFFS' PROPERTY 40

B. PLAINTIFFS HAVE A VIABLE REGULATORY TAKINGS CLAIM 47

1. THE LAW WILL INTERFERE WITH PLAINTIFFS' DISTINCT INVESTMENT-BACKED EXPECTATIONS 48

TABLE OF CONTENTS
(CONTINUED)

PAGE

2. THE LAW WILL HAVE A SIGNIFICANT ECONOMIC IMPACT ON PLAINTIFFS.....50

3. THE LAW DOES NOT MERELY ADJUST THE BENEFITS AND BURDENS OF ECONOMIC LIFE TO PROMOTE THE COMMON GOOD 51

IV. THE LAW IS VOID FOR VAGUENESS.....52

CONCLUSION.....60

STATEMENT OF RELATED CASES.....61

CERTIFICATE OF SERVICE.....63

CERTIFICATE OF COMPLIANCE.....64

TABLES OF AUTHORITIES

Page(s)

CASES

Allied Structural Steel Co. v. Spannaus,
438 U.S. 234 (1978) 27, 35

American Coal Co. v. Fed. Mine Safety & Health Review Commission,
796 F.3d 18 (D.C. Cir. 2015) 58

Arc of Cal. v. Douglas,
757 F.3d 975 (9th Cir. 2014) 1

Ass'n of Equip. Mfrs. v. Burgum,
932 F.3d 727 (8th Cir. 2019) 35, 37, 38

Belle Maer Harbor v. Charter Twp. of Harrison,
170 F.3d 553 (6th Cir. 1999) 56

Brown v. Legal Foundation of Washington,
538 U.S. 216 (2003) 46

Cartoon Network LP v. CSC Holdings, Inc.,
536 F.3d 121 (2d Cir. 2008) 18

Christie v. Nat'l Inst. for Newman Studies,
2019 WL 1916204 (D.N.J. Apr. 30, 2019) 25

Cienega Gardens v. United States,
331 F.3d 1319 (Fed. Cir. 2003) 49, 51

Coates v. City of Cincinnati,
402 U.S. 611 (1971) 53

Colony Cove Props., LLC v. City of Carson,
888 F.3d 445 (9th Cir. 2018) 49

Computer Assocs. Int'l v. Altai, Inc.,
982 F.2d 693 (2d Cir. 1992) 20

Connally v. Gen. Constr. Co.,
269 U.S. 385 (1926) 53, 59, 60

Crosby v. Nat'l Foreign Trade Council,
530 U.S. 363 (2000) 14, 27

Cycle Barn, Inc. v. Arctic Cat Sales, Inc.,
701 F. Supp. 2d 1197 (W.D. Wash. 2010) 36

Dodd v. Hood River Cty.,
136 F.3d 1219 (9th Cir. 1998) 47

Emp'rs Mut. Cas. Co. v. DGG & CAR, Inc.,
183 P.3d 513 (Ariz. 2008) 30

Energy Reserves Grp. v. Kan. Power & Light Co.,
459 U.S. 400 (1983) ..... Passim

Experian Info. Solutions, Inc. v. Nationwide Mktg. Servs.,
893 F.3d 1176 (9th Cir. 2017) 21

Facebook, Inc. v. Power Ventures, Inc.,
844 F.3d 1058 (9th Cir. 2016) 25, 26

FCC v. Florida Power Corp.,
480 U.S. 245 (1987) 46

Freightliner Corp. v. Myrick,
514 U.S. 280 (1995) 14, 15

Gen. Motors Corp. v. Romein,
503 U.S. 181 (1992) 28

Guerrero v. Whitaker,
908 F.3d 541 (9th Cir. 2018) 53, 56

Guggenheim v. City of Goleta,
638 F.3d 1111 (9th Cir. 2010) (en banc) 51

Hines v. Davidowitz,
312 U.S. 52 (1941) 27

hiQ Labs, Inc. v. LinkedIn Corp.,
273 F. Supp. 3d 1099 (N.D. Cal. 2017) 26

hiQ Labs, Inc. v. LinkedIn Corp.,
938 F.3d 985 (9th Cir. 2019) 26

Horne v. Dep't of Agric.,
576 U.S. 350 (2015) 40, 41, 45, 47

In re Dealer Mgmt. Sys. Antitrust Litig.,
362 F. Supp. 3d 558 (N.D. Ill. 2019) 25

In re Seltzer,
104 F.3d 234 (9th Cir. 1996) 39

James v. Campbell,
104 U.S. 356 (1881) 41

Johnson Controls Inc. v. Phoenix Control Sys., Inc.,
886 F.2d 1173 (1989) 20

Johnson v. U.S.,
576 U.S. 591 (2015) 53, 56

Keystone Bituminous Coal Ass'n v. DeBenedictis,
480 U.S. 470 (1987) 35

Lacey v. Maricopa Cnty.,
693 F.3d 896 (9th Cir. 2012) 12

Laurel Park Cmty. LLC v. City of Tumwater,
698 F.3d 1180 (9th Cir. 2012) 50

Lingle v. Chevron U.S.A., Inc.,
544 U.S. 528 (2005) 41, 47, 48

LL Liquor, Inc. v. Montana,
912 F.3d 533 (9th Cir. 2018) 28

Loretto v. Teleprompter Manhattan CATV Corp.,
458 U.S. 419 (1982)..... 41, 43, 44, 45

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 24

MAI Systems Corp. v. Peak Computer, Inc.,
991 F.2d 511 (9th Cir. 1993) 17, 18

McGrath v. R.I. Ret. Bd.,
88 F.3d 12 (1st Cir. 1996)..... 38

MHC Fin. Ltd. P'ship v. City of San Rafael,
714 F.3d 1118 (9th Cir. 2013) 52

Monarch Content Management LLC v. Arizona Department of Gaming.,
2019 WL 7019416 (D. Ariz. Dec. 20, 2019)..... 57

Oracle Am., Inc. v. Google Inc.,
750 F.3d 1339 (Fed. Cir. 2014) 19, 20, 21

Penn Cent. Transp. Co. v City of New York,
438 U.S. 104 (1978)..... 47, 51

Planned Parenthood Ariz., Inc. v. Humble,
753 F.3d 905 (9th Cir. 2014) 12

Playmakers Media Co.,
725 F. Supp. 2d 378 (S.D.N.Y. 2010) 25

Pure Wafer, Inc. v. City of Prescott,
845 F.3d 943 (9th Cir. 2017) 27

Ross v. City of Berkeley,
655 F. Supp. 820 (N.D. Cal. 1987)..... 36

Ruckelshaus v. Monsanto Co.,
467 U.S. 986 (1984)..... 41, 44, 45, 48

St. Mark Roman Catholic Parish Phoenix v. City of Phoenix,
2010 WL 11519169 (D. Ariz. March 3, 2010)..... 59

Stenograph L.L.C. v. Bossard Assocs., Inc.,
144 F.3d 96 (D.C. Cir. 1998)..... 17

Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.,
421 F.3d 1307 (Fed. Cir. 2005) 17

Suitum v. Tahoe Reg'l Planning Agency,
520 U.S. 725 (1997)..... 51

Sveen v. Melin,
138 S. Ct. 1815 (2018)..... 27, 28, 33, 34

Tahoe-Sierra Pres. Council, Inc. v. Tahoe Reg'l Planning Agency,
535 U.S. 302 (2002)..... 49

Taylor v. United States,
959 F.3d 1081 (Fed. Cir. 2020) 52

United States v. Nosal,
844 F.3d 1024 (9th Cir. 2016) 24

United States v. Washington,
157 F.3d 630 (9th Cir. 1998) 12

USA Recycling, Inc. v. Town of Babylon,
66 F.3d 1272 (2d Cir. 1995) 2

Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.,
455 U.S. 489 (1982)..... 57, 58

CONSTITUTIONAL PROVISIONS AND STATUTES

U.S. Const. amend. V..... 40, 46

U.S. Const. art. I, § 10, cl. 1 27

U.S. Const. art. VI, cl. 2 14

17 U.S.C. § 103 15

17 U.S.C. § 106 ..... 15, 17

18 U.S.C. § 1030(a) 23

28 U.S.C. § 1292(a)(1) 1

28 U.S.C. § 1331 1

A.R.S. § 13-803 9

A.R.S. § 28-121 9

A.R.S. § 28-4651 ..... passim

A.R.S. § 28-4653 ..... passim

A.R.S. § 28-4654 ..... 8, 9, 16, 19, 22, 30

RULES

Fed. R. App. P. 4 1

Fed. R. App. P. 28 61

Fed. R. App. P. 32 64

Fed. R. Civ. P. 12(b)(6) 12

Ninth Cir. R. 28-2.6 61

Ninth Cir. R. 28-2.7 3

Ninth Cir. R. 32-1 64

REGULATIONS

16 C.F.R. § 314.4 30

OTHER AUTHORITIES

16 Charles Alan Wright *et al*., Federal Practice and Procedure § 3937 (1977) 2

Robert F. Reilly, When Assessing Computer Software, Fair Market Value Does Not Equal Net Book Value,
23-MAR J. MULTISTATE TAX'N 6, 2013 WL 1901315 (Mar./Apr. 2013) 60

Ryan P. Bouray, CPA, and Glenn E. Richards, CPA, Accounting for external-use software development costs in an agile environment,
J. OF ACCT. (Mar. 12, 2018)..... 60

STATEMENT REGARDING ORAL ARGUMENT

Appellants respectfully request oral argument. This case involves an appeal from the district court's denial of Appellants' motion for a preliminary injunction, in which Appellants raised multiple constitutional challenges to a state law. Also at issue is the district court's decision to dismiss additional constitutional challenges to the same state law. The legal and factual issues in this appeal are complex, and the Court's evaluation of the case will be aided materially by oral argument

JURISDICTIONAL STATEMENT

District court jurisdiction. The district court had jurisdiction under 28 U.S.C. § 1331 because Plaintiffs alleged violations of the federal Constitution.

Appellate court jurisdiction. This Court has jurisdiction under 28 U.S.C. § 1292(a)(1) because Plaintiffs appeal from the district court's July 24, 2020 denial of their motion for a preliminary injunction. ER0008-0024. Plaintiffs filed a timely notice of appeal on July 30, 2020. ER0001-7; *see* Fed. R. App. P. 4(a)(1)(A).

This Court also has pendent jurisdiction over the May 20, 2020 order granting in part Defendants' motion to dismiss. ER0025-47. When an order dismisses fewer than all of the claims and arises "in connection with" a denial of a motion for injunctive relief, this Court may exercise "pendent appellate jurisdiction" if the dismissal order is "inextricably intertwined with or necessary to ensure meaningful review of the order properly before us." *Arc of Cal. v. Douglas*, 757 F.3d 975, 992-93 (9th Cir. 2014). Here, the parties briefed the motions to dismiss and for a preliminary injunction in parallel, ER0475-826, ER0905-1116, and the district court's denial of a preliminary injunction rested entirely on its determination that Plaintiffs had not shown a likelihood of success on the merits—a determination that the court necessarily reached for the earlier-dismissed claims as well. *See Douglas*, 757 F.3d at 993.

The exercise of pendent jurisdiction would also serve judicial economy, because the motion to dismiss raises purely legal issues that this Court will address under the same standard as in a post-final-judgment appeal. Thus, "[o]n appeal from grant or denial of a preliminary injunction, … it may make excellent sense to determine whether the complaint states a claim on which relief can be granted." *USA Recycling, Inc. v. Town of Babylon*, 66 F.3d 1272, 1294 (2d Cir. 1995) (quoting 16 Charles Alan Wright *et al*., Federal Practice and Procedure § 3937 (1977)).

STATEMENT OF THE ISSUES PRESENTED

1. Whether Arizona HB 2418 ("the Law") is preempted by the Copyright Act because the Law allows third parties to copy Plaintiffs' creative works without their permission in irreconcilable conflict with the federal protections afforded copyright holders.

2. Whether Plaintiffs stated a claim that the Law is preempted by the Computer Fraud and Abuse Act ("CFAA") where the Law authorizes third parties to access Plaintiffs' computer systems without their permission in irreconcilable conflict with the CFAA's prohibition against unauthorized, third-party computer access.

3. Whether the Law violates the Contracts Clause because it eliminates or severely restricts Plaintiffs' existing contract rights by giving auto dealers the unilateral power to authorize third parties to access Plaintiffs' systems, which in turn

jeopardizes data security by creating more connection points for hackers to exploit, and there is no evidence that the Law serves a significant and legitimate public purpose.

4. Whether the Law violates the Takings Clause because it permits third parties to access Plaintiffs' computer systems and occupy Plaintiffs' databases by writing data to those systems without affording Plaintiffs just compensation.

5. Whether Plaintiffs stated a claim that the Law is unconstitutionally vague where it leaves Plaintiffs to guess what prohibited "unreasonable" conduct means or how to calculate their "direct costs," at risk of criminal penalties if Plaintiffs guess wrong.

STATEMENT REGARDING STATUTORY ADDENDUM

A statutory addendum containing excerpts of relevant authority, as required by Ninth Circuit Rule 28-2.7, is included as an addendum to this brief.

STATEMENT OF THE CASE

A. The Dealer Management System

Plaintiffs CDK Global, LLC ("CDK") and The Reynolds & Reynolds Company ("Reynolds") own and operate natively developed proprietary computer systems known as Dealer Management Systems ("DMSs") that automobile dealerships license to manage their businesses. ER0943-944 (¶¶ 4-6); ER0959 (¶ 2); *see also* ER0304 (49:4-8). Plaintiffs have invested hundreds of millions of dollars and countless human hours into developing, operating, and securing their respective

systems. ER0945 (¶ 12); ER0948 (¶ 29); ER0962 (¶¶ 10-12); ER0964 (¶ 17); ER0967 (¶ 29).

These computer systems consist of both hardware and copyright-protected software components, including millions of lines of code performing functions such as entering customer information, updating vehicle records, and transmitting financial data between dealers and credit bureaus. ER0943 (¶¶ 5-6); ER0959-960 (¶¶ 3, 5-6); ER0962-963 (¶¶ 13-14). A user cannot access or use a DMS without creating copies of and executing Plaintiffs' computer programs. *See* ER0963 (¶ 14); *see also* ER0560 (¶ 8); ER0566 (¶ 5).

Plaintiffs have compiled vast amounts of information in their DMSs, including confidential consumer data and other information obtained from dealers, manufacturers, credit bureaus, and various third parties. ER0944-945 (¶¶ 9-10); ER0961-962 (¶¶ 8-9); ER0304 (50:10-15); ER0305 (53:2-54:13). Plaintiffs also add their own proprietary data to these compilations. ER0304-305 (52:24-53:7); ER0253 (139:18-24). In addition to selecting the types of data compiled in their DMSs, Plaintiffs apply their own "business rules" to structure and organize this data in creative ways. *See* ER0304 (50:16-52:2). Plaintiffs' DMSs thus contain hundreds of thousands of inter-related data fields. *See* ER0304-305 (52:5-53:22); ER0251-252 (131:3-132:10).

Plaintiffs author the computer programs in their systems, including the code that created these databases, and they operate (or contract for) the computer servers that house the databases. *See* ER0303-304 (46:5-21, 47:21-48:6, 48:17-49:8; 50:2-15); ER0252 (132:4-23). They also maintain these databases, collect, organize, and enrich the data they house, and render the data in a form useful to their dealer clients. ER0308 (67:16-68:10); ER0252 (133:8-14); ER0565.

To secure their systems, protect their intellectual property, and fulfill legal and contractual obligations to secure data compiled on their databases, Plaintiffs license access to their computer systems and copyright-protected software through detailed and heavily negotiated contracts that prohibit their dealer licensees from granting third parties access to the DMS without Plaintiffs' authorization. ER0945-946 (¶¶ 13-16), ER1233-1246; ER0963-964 (¶¶ 15-16), ER0976-977; ER0979-1038. For example, CDK's Master Service Agreement provides that a dealer "IS NOT AUTHORIZED TO CAUSE OR PERMIT ANY THIRD PARTY SOFTWARE TO ACCESS THE [CDK DEALER MANAGEMENT SYSTEM] EXCEPT AS OTHERWISE PERMITTED BY THIS AGREEMENT." ER1249 (§ 4(B)); *see also* ER1249-1250 (§ 4(D)), ER0945-946 (¶ 14). Similarly, each dealer who signs the Reynolds Master Agreement agrees "not to disclose or provide access to any Licensed Matter or non-public portions of the Site to any third party, except [dealer] employees who have a need for access to operate [the] business and who

agree to comply with [the dealer's] obligations under this Section 1[.]" ER0976 (§ 1(c)); ER0946 (¶14). Reynolds' Customer Guide further states that dealers "shall not copy, reproduce, distribute, or in any way disseminate or allow access to or by third parties." ER1000; *see also* ER0963-964 (¶ 15); ER0998-999. Both CDK and Reynolds agree in their licensing agreements to implement and maintain appropriate safeguards pursuant to their federal obligations under the Gramm-Leach-Bliley Act and Safeguards Rule. ER0945 (¶¶ 13-14); ER0977 (§ 5(f)); ER0962-963 (¶¶ 10, 15); ER0988.

In addition to licensing new car dealers, Plaintiffs also license third parties to interface with Plaintiffs' computer systems. These third parties, including external software vendors, seek to access and leverage the functionality of Plaintiffs' DMSs to provide other applications to dealers. ER0946-949 (¶¶ 17-31) (describing CDK's Partner Program, formerly known as the 3PA Program); ER0964-967 (¶¶ 17-28) (describing Reynolds's RCI Program); ER0308 (67:4-8); ER0251 (131:22-24). Plaintiffs build custom interfaces specific to each vendor's intended use of the DMS, and these interfaces can take several months and cost hundreds of thousands of dollars for Plaintiffs to author and develop. ER0255 (146:16-21). The license agreements with these vendors include restrictions on how the vendors can access and use Plaintiffs' systems and software, and require them to pay market-based fees for access to Plaintiffs' DMSs. ER0947 (¶ 21), ER1235-1236 (§§ 2(a)-(e)); ER1237-

1241 (§§ 3, 4, 5); ER0965 (¶ 21); ER1041-1046 (§§ 1.9, 1.10, 2.2, 2.4, 2.5, 2.7). In CDK's case, revenue associated with these agreements accounts for five percent of its total revenue (i.e., tens of millions of dollars per quarter). *See* ER0258-259 (159:5-161:14).

B. The Law

Arizona HB 2148 (the "Law") gives Arizona dealers the right to grant unlicensed third parties—so-called "authorized integrators"—access to *Plaintiffs*' computer systems and the right to share *Plaintiffs*' data compilations. *See* A.R.S. § 28-4651.1 (defining "authorized integrator" as "a third party with whom a dealer enters into a contractual relationship to perform a specific function for a dealer that allows the third party to access protected dealer data or to write data to a dealer data ststem, or both, to carry out the specified function.").

The Law prohibits DMS providers from taking "*any action* by contract, technical means or otherwise to prohibit or limit a dealer's ability to protect, store, copy, share or use protected dealer data." A.R.S. § 28-4653.A.3 (emphasis added). The Law defines "protected dealer data" broadly to include consumer data, vehicle diagnostic data, and "other data that relates to a dealer's business operations in the dealer's dealer data system." *Id.* § 28-4651.7. Both Plaintiffs' and Defendants' witnesses agree that this definition covers "[v]irtually all" data processed and compiled in Plaintiffs' DMSs. *See* ER0304 (52:21-23); ER0254 (140:18-23);

ER0128 (370:17-22).

The Law specifically forbids DMS providers from "imposing any fee or other restriction on the dealer or an authorized integrator for accessing or sharing protected dealer data or for writing data to a dealer data system." A.R.S. § 28-4653.A.3(a). The Law defines "fee" as "a charge for allowing access to protected dealer data beyond any direct costs," without defining "direct costs." *Id.* § 28-4651.5. As such, the Law mandates that DMS providers provide at-cost access to their computer systems and copyright-protected software.

The Law further prohibits DMS providers from placing an "unreasonable restriction on integration by an authorized integrator." *Id.* § 28-4651.3.A.3(b). The Law lists six examples of an "unreasonable restriction," four of which use the word "unreasonable." *Id.*

To comply with the Law, DMS providers must "make available a standardized framework for the exchange, integration and sharing of data." *Id.* § 28-4654.A.1. Specifically, DMS providers must provide "authorized integrators" with "access to open application programming interfaces" or "a similar open access integration method." *Id.* § 28-4654.A.2. An "authorized integrator" may then integrate with a DMS provider's computer system and use a DMS provider's copyright-protected software to "access, use, store, or share protected dealer data or any other data from a dealer data system" to whatever extent allowed by the Arizona dealer. *Id.* § 28-

4654.B.1.

As part of A.R.S. Title 28, the Law imposes criminal penalties on DMS providers that could exceed $16,000 per day for non-compliance. *See* A.R.S. §§ 13-803, 28-121.

C. The Impact Of Compliance With The Law On DMS Providers

Compliance with the Law requires DMS providers to develop new software to allow unlicensed third parties that Plaintiffs have not chosen to do business with to create and execute unauthorized copies of Plaintiffs' copyright-protected DMS software. ER00952 (¶ 42); ER00969 (¶ 37). Indeed, copyright-protected DMS software is always copied into memory and executed to perform a requested function, regardless of what method is used to access the system or submit a request to extract, insert, or modify data. ER0309 (69:18-70:9); ER0560-561 (¶¶ 8, 10, 14, 15); ER0566 (¶ 5).

Likewise, the application programming interfaces ("APIs") that DMS providers must create under the Law are original works of creative expression. ER0559 (¶ 4). And the fact that the APIs mandated by the Law require use of a "standardized framework" to exchange data with so-called "authorized integrators" does nothing to change that fact. ER0559 (¶ 7); *see also* ER0308-309 (68:19-69:8, 69:9-12). To implement these APIs, any third party using the API's specification must copy that creative work into their software. *See* ER0559-560 (¶¶ 5, 9); ER0309

(69:9-17).

Additionally, it is impossible for Plaintiffs to ascertain what "reasonable" technical restrictions, if any, it can incorporate into any APIs it must develop to comply with the Law. ER0951-952 (¶¶ 36, 38, 41); ER0970-972 (¶¶ 39–46). Even Defendants' witnesses could not agree as to what would be "reasonable." Defense witness Alan Andreu testified that Plaintiffs' current restrictions, including basic security measures like CAPTCHA logins and restrictions on automated access, are unreasonable. *See* ER0122-126 (346:8-362:7); *see also* ER0124-125 (352:3-15, 357:20-358:11). But Defendants' cybersecurity expert, Hoyt Kesterson, testified that "the exact same types of controls that are already in place" in Plaintiffs' systems could all be continued under the Law. ER0194 (300:6-22); *see also* ER0188-189 (279:14-17, 281:11-18, 282:14-16); ER0193-194 (299:14-300:11, 302:18-25); ER0117-118 (325:12-22, 330:17-19). Rather than define the contours of what would be "reasonable" under the Law, Kesterson later remarked: "I leave it to the man to my left [the judge] to define what reasonable is. That's what judges do." ER0120 (337:17-19).

Regardless of one's definition of "reasonable," compliance with the Law would make it impossible for Plaintiffs to safeguard confidential consumer and proprietary data. ER0951-952 (¶¶ 36, 38, 41); ER0970-972 (¶¶ 39–46). Compliance would make "every single data element stored or processed on the Reynolds DMS

… at greater risk of breach." ER0970 (¶ 39); *see also* ER0950-952 (¶¶ 35-42) (describing myriad ways that Law undermines cybersecurity of CDK's DMS); ER0309 (72:5-18).

D. Procedural Background Of The Case

On July 29, 2019, Plaintiffs filed a complaint against Mark Brnovich, Attorney General of the State of Arizona, and John S. Halikowski, Director of the Arizona Department of Transportation, challenging the constitutionality of the Law. ER1117-1179. On September 5, 2020, the Arizona Automobile Dealers Association ("AADA")—the organization that lobbied for passage of the Law—filed a Motion to Intervene as a Defendant, which was granted on September 12, 2019. ER0852-903; ER0850-85.

On August 23, 2019, Plaintiffs filed a motion for a preliminary injunction to enjoin enforcement of the Law. ER0905-1116. The district court granted a stipulation on September 4, 2019, to stay enforcement of the Law during the pendency of that motion. ER0904.

On May 20, 2020, the court dismissed certain of Plaintiffs' claims, including that the Law was preempted by the Federal Consumer Fraud and Abuse Act (CFAA) and was void for vagueness. ER0025-47. The court, however, sustained Plaintiffs'

copyright preemption claim and claims based on the Contracts and Takings Clauses.[1] *Id.*

On June 2 and 3, 2020, the district court held a preliminary injunction hearing with respect to the remaining claims. ER0344; ER0238. On July 24, 2020, the district court denied that motion. ER0008-24.

Plaintiffs now appeal the district court's order on the motion to dismiss and its order denying a preliminary injunction.

STANDARD OF REVIEW

This Court "review[s] the district court's denial of a preliminary injunction for abuse of discretion." *Planned Parenthood Ariz., Inc. v. Humble*, 753 F.3d 905, 911 (9th Cir. 2014). The district court abuses its discretion when its decision "is based on an error of law or a clearly erroneous factual finding." *United States v. Washington*, 157 F.3d 630, 642 (9th Cir. 1998).

This Court "review[s] de novo the district court's dismissal for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6)." *Lacey v. Maricopa Cnty.*, 693 F.3d 896, 911 (9th Cir. 2012) (en banc).

SUMMARY OF THE ARGUMENT

The district court's order denying Plaintiffs' motion for a preliminary

[1] On April 2, 2020, the district court dismissed Plaintiffs' claims against Arizona Department of Transportation Director John S. Halikowski for lack of subject matter jurisdiction. ER0469-474. Plaintiffs are not appealing that Order.

injunction should be vacated. That order rested solely on the court's conclusion that Plaintiffs had not established a likelihood of success on their claims. The court, however, ignored uncontroverted evidence and misapplied the relevant legal standards. Plaintiffs need only prevail on one claim for this Court to remand the matter for further proceedings on their preliminary injunction motion. As shown below, they should prevail on five claims.

The court misapplied the relevant law governing two different federal preemption claims. First, Plaintiffs established that they own copyrights in their own computer programs, application programming interfaces ("APIs"), and data compilations—all original, creative works. As such, the Copyright Act grants Plaintiffs the exclusive rights to reproduce and distribute copies of those works. The Law, however, vitiates these exclusive rights, giving Arizona automobile dealers and third-party "authorized integrators" the right to access Plaintiffs' computer systems and create unlicensed copies of the protected works. Second, the CFAA's text (and purpose) prohibit a third party from accessing a computer system without the system owner's permission. The Law overrides that federal statutory right by granting permission to third parties as a matter of state law. The conflict is irreconcilable.

Plaintiffs are also likely to succeed on the merits of their Contracts Clause claim. The Law impairs Plaintiffs' contractual right to determine who may access their systems by vesting unilateral authority in auto dealers to permit third parties to

integrate into the DMSs. The Law also impairs Plaintiffs' contractual obligation to protect the security of data in the DMSs by creating more integration points that hackers can exploit. There is no significant and legitimate public purpose justifying these impairments. The Law was passed to benefit a special interest group—auto dealers—not to remedy a broad social or economic problem.

Plaintiffs are likely to succeed on their takings claim, as well. The Law permits third parties to access and write data to the DMSs without Plaintiffs' permission and without allowing Plaintiffs to obtain market value for their DMS integration services. That physical occupation of Plaintiffs' computer systems is a *per se* taking.

Finally, Plaintiffs are likely to succeed on their claim that the Law is unconstitutionally vague. The Law criminalizes "unreasonable" conduct but gives Plaintiffs no notice of what is "unreasonable" and what is permissible. The Law also criminalizes charging anything beyond "direct costs" for integration services but again gives Plaintiffs no notice how to calculate permissible "direct cost" charges.

ARGUMENT

I. The Law Is Preempted.

"A fundamental principle of the Constitution is that Congress has the power to preempt state law." *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372 (2000) (citing U.S. Const. art. VI, cl. 2). Congress may do so expressly or implicitly

where "state law is in actual conflict with federal law." *Freightliner Corp. v. Myrick*, 514 U.S. 280, 287 (1995). Regarding the latter, conflict preemption voids any state law that "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Id*. Plaintiffs are likely to succeed on their claim that the Law stands as an obstacle to two federal laws and is thus preempted.

A. The Law Conflicts With The Copyright Act.

Plaintiffs are likely to succeed on their claim that the Law conflicts with the Copyright Act by contravening the "exclusive rights" granted Plaintiffs under 17 U.S.C. § 106 "to reproduce" and "distribute copies" of their copyrighted works. The Law grants Arizona automobile dealers and so-called "authorized integrators" the right to access Plaintiffs' computer systems and create unlicensed copies of Plaintiffs' copyrighted works, including: (1) Plaintiffs' DMS computer programs; (2) APIs Plaintiffs are compelled to author under the Law; and (3) Plaintiffs' data compilations, which are protected by 17 U.S.C. § 103. The district court erred by misapplying governing law and disregarding undisputed facts concerning the unlicensed copying authorized by the Law in contravention of the Copyright Act.

1. The Law vitiates Plaintiffs' exclusive rights in their copyrighted DMS software.

Plaintiffs have invested hundreds of millions of dollars in developing their DMS software programs. ER0962 (¶ 12); ER0307 (62:3-63:13). They authored these programs "from a concept standpoint, to design, to the actual coding and testing of

the software." ER0304 (49:4-8); *see also* ER0252 (132:4-10). Plaintiffs seek a return on their significant investments by licensing their copyrighted software and associated systems to automobile dealers. *See, e.g.*, ER0959 (¶ 3); ER0943 (¶ 4); ER0252 (132:14-23). Plaintiffs also license third-party application providers who seek to "integrate" with the DMS software to provide their own applications and services. ER0965 (¶ 21); ER1040-1067; ER0946-947 (¶¶ 17, 21); ER1233-1246.

Under the Law, Plaintiffs must grant access to their computer programs to *any* third party an Arizona dealer designates as an "authorized integrator." And Plaintiffs must provide an "open access integration method"—such as an "open" API—allowing those "authorized integrators" to "integrate" with Plaintiffs' computer systems. A.R.S. § 28-4654.A.2. An "authorized integrator" may then use Plaintiffs' computer programs to "access, use, store, or share protected dealer data or any other data from a dealer data system" to whatever extent allowed by the Arizona dealer that authorized access. *Id.* § 28-4654.B.1. Plaintiffs may not place any "unreasonable restriction" on such "integration." *Id.* § 28-4653.A.3(b).

The undisputed evidence shows that every time a third party uses an "open access integration method" to integrate with Plaintiffs' systems, that party causes a copy of Plaintiffs' software to be created in the memory of Plaintiffs' computers. *See, e.g.*, ER0560-561 (¶¶ 10, 14); ER0309 (69:18-70:9). Causing a copy of a computer program to be loaded into memory creates a "copy" of that program within

the meaning of § 106 of the Copyright Act. The Copyright Act grants copyright owners the exclusive right "*to reproduce* the copyrighted work," regardless of who obtains possession of that reproduction. 17 U.S.C. § 106(1).

Indeed, this Court held in *MAI Systems Corp. v. Peak Computer, Inc.* that the loading of copyrighted computer software from a storage medium into a CPU "causes a copy to be made" under the Copyright Act. 991 F.2d 511, 518 (9th Cir. 1993); *see also Stenograph L.L.C. v. Bossard Assocs., Inc.*, 144 F.3d 96, 100 (D.C. Cir. 1998) (loading program into memory creates copy under Copyright Act); *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1311 (Fed. Cir. 2005) (same).

In its Order denying Plaintiffs' motion for preliminary injunction, the district court did not address *MAI* and disregarded the unrebutted evidence of copying. The district court instead found that Plaintiffs can comply with the Law without copying because they can provide access to their systems through APIs that "do[] not copy software from [the DMS provider's] DMS at all." ER0014; *see also* ER0012 (n.8); ER0014. But this misses the point: Plaintiffs never argued that APIs are themselves copies of DMS computer programs. Plaintiffs asserted—and the unrebutted testimony established—that a third party, *using an API*, sends commands that cause unlicensed copies of the DMS software to be made in memory and executed on Plaintiffs' servers, violating the exclusive rights granted Plaintiffs under the

Copyright Act. ER0560-561 (¶¶ 10, 14); ER0309 (69:18-70:9); ER0245 (105:22-107:14).

The district court also erred in holding that the Law does not conflict with the Copyright Act because "authorized integrators" do not "*obtain* a copy" of Plaintiffs' computer programs. ER0015. The relevant inquiry, however, is not *where* the copy resides, but rather whether it is made and *who* causes it to be made. Indeed, this Court has held that a party infringes the rights granted under the Copyright Act by causing copies to be made on systems belonging to third parties. For example, the defendant in *MAI Systems* engaged in copyright infringement by causing a copy of software to be loaded into the memory of another's computer. *See MAI Sys. Corp.*, 991 F.2d at 518; *see also id.* at 524 (affirming permanent injunction prohibiting infringer from "*causing* [a computer program] to be loaded, *directly or indirectly*" into RAM) (emphasis added).

Similarly, the Second Circuit held in *Cartoon Network LP v. CSC Holdings, Inc.* that a cable subscriber infringes a copyright when the subscriber causes a television program to be copied in memory on the cable system's server. 536 F.3d 121, 130 (2d Cir. 2008); *see also id.* at 134 ("copies produced by the RS-DVR system are 'made' by the RS-DVR customer"). The court explained that the party that *causes* a copy to be made—not the party possessing the copy—is the infringer. *Id.* at 131.

2. The Law vitiates Plaintiffs' exclusive rights in APIs they author.

The Law requires Plaintiffs to create "open" APIs and provide them for use by "authorized integrators." A.R.S. § 28-4654.A.2. As the Federal Circuit has held, "API packages … are entitled to copyright protection." *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1381 (Fed. Cir. 2014). This is because an API can qualify as an original work of expression reflecting the author's creativity. *See id.* at 1356. Here, the unrebutted evidence confirms the creativity of the APIs Plaintiffs must author to permit integration. ER0308-309 (68:19-69:17); *see also* ER0559 (¶ 4); ER0567 (¶ 9).

The unrebutted evidence also establishes that "authorized integrators" must copy portions of the APIs to integrate with Plaintiffs' systems under the Law. ER0561 (¶ 14). Indeed, the entire purpose of an API is to instruct integrators on what they must include in their code to access Plaintiffs' systems (e.g., "the field names, the specifications, the data names, and the attributes" of the APIs). ER0308-309 (68:19-69:17); *see also* ER0559 (¶ 4); ER0787 (¶ 13).

In denying the preliminary injunction, the district court disregarded the unrebutted testimony concerning the creative elements of Plaintiffs' APIs and the third-party copying of those APIs that the Law authorizes in contravention of § 106 of the Copyright Act. Instead, the district court held that there was no conflict with federal law because APIs used to access a DMS do not copy "source code" and,

therefore, are distinguishable from the APIs in *Oracle*. ER0014-15.

The district court's decision is wrong as a matter of law in at least two respects. First, without citation to the Copyright Act or relevant case law, the court held that copyright protection for APIs extends only to "source code" and not to other creative elements of APIs. In fact, copyright protection extends beyond "source code" to cover other elements of an API. For example, *Oracle* recognizes that the Copyright Act protects the "structure, sequence and organization" of API packages. *Oracle*, 750 F.3d at 1354; *see, e.g.*, *Computer Assocs. Int'l v. Altai, Inc.*, 982 F.2d 693, 702 (2d Cir. 1992); *Johnson Controls Inc. v. Phoenix Control Sys., Inc.*, 886 F.2d 1173, 1175-76 (9th Cir. 1989).

Second, the district court misapplied *Oracle*, which held that the Copyright Act protects the "declaring code" of an API. While ostensibly relying on *Oracle*'s reference to "code" (ER0015), the district court failed to appreciate that the "declaring code" in *Oracle* is closely analogous to the API "schema" that will be copied under the Law. Indeed, uncontroverted testimony establishes that integrators would "have to copy the field names, the specifications, the data names and the attributes from the [API] document into their source code into how they call [the DMS servers]." ER0309 (69:13-17). This means that, for third-party integrators to interface with the DMS servers and read data from or write data to those servers, they must copy syntax developed by Plaintiffs to send commands to Plaintiffs'

computer systems to run the corresponding functions on those servers and have them return the requested information. This is equivalent to the "declaring code" found protected in *Oracle*, which programmers used to "command the computer to execute the associated implementing code, which gives the computer the step-by-step instructions for carrying out the declared function." *See Oracle*, 750 F.3d at 1349. Here, where the unrebutted evidence confirms the creativity of the APIs that Plaintiffs must author to permit integration, and where the Law would necessarily result in unauthorized reproduction of these APIs by third-party integrators, the Law conflicts directly with the Copyright Act.

3. The Law vitiates Plaintiffs' exclusive rights in their data compilations.

The Law also conflicts with the Copyright Act because the Law grants dealers and their "authorized integrators" the right to copy and distribute Plaintiffs' copyrighted data compilations.

Data compilations are protected under § 103 of the Copyright Act "as long as there is creativity in the selection, arrangement, or coordination of the facts." *Experian Info. Solutions, Inc. v. Nationwide Mktg. Servs.*, 893 F.3d 1176, 1184 (9th Cir. 2017); *see id.* at 1185 (list of names correlated with addresses sufficient for copyright protection). There is no dispute that Plaintiffs have creatively selected, arranged, and coordinated the data they have compiled in their DMSs from a wide variety of sources, including dealers, consumers, auto manufactures, and financial

institutions. ER0944 (¶ 9); ER0565 (¶ 3); ER0305 (53:12-22). Plaintiffs then applied their own "business rules" to structure and organize the data in creative ways. ER0304 (50:16-52:2).

Under the Law, Arizona dealers and their "authorized integrators" are granted the right (in direct contravention of the Copyright Act) to reproduce and distribute copies of Plaintiffs' data compilations, *i.e.*, to copy and share "protected dealer data." *See, e.g.*, A.R.S. §§ 28-4654.B.1, 28-4653A.3(a). The Law defines "protected dealer data" to include all "data that relates to a dealer's business operations," *id.* § 28-4651(7)(c), that is, "[v]irtually all" the data compiled in Plaintiffs' DMSs. ER0304 (52:21-23); *see also* ER0254 (140:18-23); ER0128 (370:17-22). The Law therefore gives third parties the right to copy and share "virtually all" of Plaintiffs' data compilations.

The district court side-stepped this conflict with the Copyright Act by holding that A.R.S. § 28-4654.A.1 requires Plaintiffs to apply a "standardized framework." The court explained that Plaintiffs "will not use their own organization and structure at all, but rather a 'standardized' structure used by all dealer data vendors who want to do business in Arizona." ER0015. But this theory, which Defendants never raised, is clearly incorrect. The Law's reference is to a "standardized" *communications* framework—*i.e.*, a framework for the "exchange, integration and sharing of data." A.R.S. § 28-4654.A.1. This "standardized framework" does not alter the scope of

the "protected dealer data" that can be copied and distributed under the Law; nor does this framework in any way change the content, organization, or layout of the data and the creative choices embedded therein.[2] It was legal error for the district court to hold otherwise.

B. The District Court Erred In Dismissing Plaintiffs' CFAA Preemption Claim.

The district court erred both in dismissing Plaintiffs' CFAA claim and in denying a preliminary injunction on the basis of their CFAA claim. The CFAA makes it unlawful to "knowingly access[] a computer without authorization" or to "excee[d] authorized access." 18 U.S.C. § 1030(a). Under the Law, however, a DMS provider may not "prohibit[] a third party … that the dealer has identified as one of its authorized integrators from integrating into that dealer's dealer data system." A.R.S. § 28-4653.A.3(b). The Law also bars DMS owners—like Plaintiffs—from placing any "unreasonable" restrictions "on the scope or nature of the data that is shared with an authorized integrator," or on "the ability of the authorized integrator to write data to a dealer data system." *Id*. § 28-4653.A.3(b)(i), (ii). The Law thus purports to allow *dealers*, rather than DMS providers, to authorize access to the DMS—in square conflict with the exclusive federal right the CFAA gives computer

[2] Because no party advanced this theory, there are no facts in the record supporting the district court's conclusion that the "standard framework" would somehow cleanse creative elements from Plaintiffs' data compilations when dealers and third-party integrators copy those compilations.

system owners to determine who may access and alter data or processes on their systems.

1. The CFAA vitiates Plaintiffs' right to determine who is authorized to access their computer systems.

The district court dismissed the CFAA preemption claim on the grounds that the CFAA "criminalizes accessing information without authorization in protected computers" but supposedly "does not limit how access might be authorized." ER0030. Instead, the court reasoned, the CFAA "leaves it to authority external to the statute itself—such as state law—to determine what is authorized or not." *Id*. But the district court cited no authority for this proposition, which is directly contrary to the text of the statute, its legislative purpose, and case law.

First, this Court has rejected the conclusion that someone other than the computer system owner can "authorize" third parties to access the system. Rather, the CFAA grants computer owners "*exclusive* discretion" to determine who can access their systems. *United States v. Nosal*, 844 F.3d 1024, 1036 (9th Cir. 2016) (emphasis added); *see also id*. at 1052 (Reinhardt, J., dissenting) (recognizing majority's holding that "authorization can be given only by the system owner"). *Nosal* built on the Court's earlier holding in *LVRC Holdings LLC v. Brekka*, which held that "[t]he plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer [*i.e.*, the system owner]." 581 F.3d 1127, 1134-35 (9th Cir. 2009). In fact, *Brekka* affirmatively rejected the theory that state

law is relevant to the authorization inquiry. *Id*. ("Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty.").

Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016), also controls here. In *Power Ventures*, this Court explained that the owner of the computer system (Facebook) could deny access to the defendant (the Power social network) even when another party (Facebook users) purported to grant the defendant "authorization." *Id*. at 1067-68. That Power had permission to access Facebook from Facebook's users was irrelevant. What mattered was that, even after Facebook made clear that the access was unauthorized, Power "continued to access Facebook's data and computers without *Facebook's* permission." 844 F.3d at 1068 (emphasis added).[3]

Second, the district court's analogy to "breaking and entering" (ER0030) fails. Under the district court's construction of the CFAA, if a watch left with a bank for safekeeping is being stored in the bank's vault, the watch's owner could authorize a

[3] Courts outside the Ninth Circuit are in accord. *See, e.g., In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d 558, 570 (N.D. Ill. 2019) ("the 'authorization' required for lawful access under the CFAA must come from the owner of the computer system"); *Christie v. Nat'l Inst. for Newman Studies*, 2019 WL 1916204, at *7 (D.N.J. Apr. 30, 2019) (same); *Univ. Sports Publ'ns. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (holding that "the term 'exceeds authorized access'" as used in the CFAA "applies to authorized users who cross boundaries set by the system owner").

third party to remove it from the bank without the bank's permission. In *Power Ventures*, however, this Court recognized that that is not the law. *See* 844 F.3d at 1068 (using analogy involving jewelry in a safe deposit box). Because the Law purports to give dealers the right to authorize third parties to access the DMS without the DMS provider's permission, the statute is preempted.

2. The district court erred in reading the CFAA "narrowly."

The district court also reasoned that Plaintiffs' preemption claim would "expand the CFAA beyond its 'narrow' aim" of deterring cybercriminals. ER0031. According to the district court, a "broad reading" of the CFAA might "stifle the dynamic evolution and incremental development of state and local laws," which Congress "could not have intended." *Id.* (citing *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017)). But in affirming the lower court decision in *hiQ Labs*, this Court said nothing about this supposed concern. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019). Instead, the Court relied solely on the meaning of "authorization" under the statute.

Moreover, Congress need not state its intent to preempt such state laws expressly. As this Court has noted, the CFAA "prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use"—full stop. *Power Ventures*, 844 F.3d at 1065. Because the Law purports to override this prohibition, Congress did not need to express its "intent" to preempt such a law

specifically. Whenever state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," it is preempted. *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941); *accord, e.g.*, *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 373 (2000).[4]

II. The Law Violates The Contracts Clause.

Plaintiffs are likely to succeed on their claim that the Law violates the Contracts Clause. The Constitution prohibits a state from passing any "[l]aw impairing the [o]bligation of [c]ontracts." U.S. Const. art. I, § 10, cl. 1. This Clause "applies to any kind of contract" and "restricts the power of States to disrupt contractual arrangements." *Sveen v. Melin*, 138 S. Ct. 1815, 1821 (2018). The Framers placed "high value … on the protection of private contracts" because contracts "enable individuals to order their personal and business affairs according to their particular needs and interests." *Allied Structural Steel Co. v. Spannaus*, 438 U.S. 234, 245 (1978). "Once arranged, those rights and obligations are binding under the law, and the parties are entitled to rely on them." *Id*.

The Clause subjects state laws changing the enforceability of contract provisions to a two-part test. *Pure Wafer, Inc. v. City of Prescott*, 845 F.3d 943, 952

[4] The district court also noted that Plaintiffs had not cited any case in which the CFAA preempted a state statute. ER0031. But until recently, no state claimed the right to authorize third parties to access private computer systems protected by federal law.

(9th Cir. 2017). First, the Court asks "whether the state law has operated as a substantial impairment of a contractual relationship." *Sveen*, 138 S. Ct. at 1821-22 (internal quotations omitted). Second, if a substantial impairment exists, the court determines "whether the state law is drawn in an appropriate and reasonable way to advance a significant and legitimate public purpose." *Id*. at 1822. "[T]he level of scrutiny to which the legislation will be subjected" under the second part "increase[s]" as "[t]he severity of the impairment" does. *Energy Reserves Grp. v. Kan. Power & Light Co.*, 459 U.S. 400, 411 (1983).

A. The Law Substantially Impairs Plaintiffs' Contracts.

The test for substantial impairment examines "'whether there is a contractual relationship, whether a change in law impairs that contractual relationship, and whether the impairment is substantial.'" *LL Liquor, Inc. v. Montana*, 912 F.3d 533, 537 (9th Cir. 2018) (quoting *Gen. Motors Corp. v. Romein*, 503 U.S. 181, 186 (1992)). The first part of the test is satisfied because Plaintiffs have entered into contracts with dealers and third-party vendors. ER0976-1067; ER1233-1256.

Moreover, the Law substantially impairs those contracts. In evaluating substantial impairment, the court "consider[s] the extent to which the law undermines the contractual bargain, interferes with a party's reasonable expectations, and prevents the party from safeguarding or reinstating his rights." *Sveen*, 138 S. Ct. at 1822. The Law does all of these things.

1. The Law undermines Plaintiffs' contractual bargains.

The Law impairs Plaintiffs' contracts with dealers by negating the contract provisions giving Plaintiffs, rather than dealers, the right to authorize access to their DMSs. It also impairs the provisions requiring Plaintiffs to protect the sensitive data maintained on the DMS because, to comply with the "open" access the Law demands, Plaintiffs must, *inter alia*, create additional connection points that hackers can exploit, thereby exposing this sensitive data to unauthorized access. The Law also impairs the provisions in Plaintiffs' contracts with third-party application providers prohibiting those third parties from accessing the DMS in any manner or for any reason other than as set forth explicitly in those contracts and requiring integrators to pay market-based fees for integration with the DMS.

Plaintiffs' contracts with dealers expressly limit access to Plaintiffs' DMSs and require dealers to obtain approval before allowing a third party to access, use, or modify the system. *See supra* pp. 5-6. The Law permits dealers to violate these agreements by prohibiting Plaintiffs from "imposing any … restriction on the dealer or an authorized integrator for accessing or sharing protected dealer data or for writing data to a dealer data system." A.R.S. § 28-4653.A.3(a). The Law also forbids Plaintiffs from prohibiting a third party chosen by a dealer "from integrating into the dealer's dealer data system." *Id.* § 28-4653.A.3(b). By allowing dealers to choose who may access and write data to Plaintiffs' DMSs, the Law nullifies the contractual

provisions—negotiated at arm's length—that prohibited dealers from conferring rights of access and use to third parties.

The district court discounted this impairment because the Law "does not require direct access to Plaintiffs' DMSs, but rather access to an API as mandated by § 28-4654."[5] ER0017. But this implicitly rewrites the DMS licensing agreements to bar only unauthorized "direct" access—a violation of basic principles of contract construction. *See Emp'rs Mut. Cas. Co. v. DGG & CAR, Inc.*, 183 P.3d 513, 518 (Ariz. 2008). Neither CDK's nor Reynolds's contracts with its dealers differentiate between "direct" and "indirect" access: either requires approval by CDK or Reynolds, respectively.

The Law also impairs Plaintiffs' ability to comply with their contractual data security obligations. CDK's MSA states that "to the extent it is a Service Provider" to the dealer under the FTC's Safeguards Rule, 16 C.F.R. § 314.4(d)(1), (2), CDK will "implement and maintain appropriate safeguards as CDK may determine to be reasonably necessary to protect the confidentiality" of non-public information in its possession and control that was provided by the dealer. ER1251. Reynolds' Customer Guide contains similar language. ER0988. The system access required by

[5] The district court repeated the point that integrators will not access the "'structure' or 'organization' of Plaintiffs' data" when they integrate under the Law. ER0017. That assertion has no evidentiary support, as noted above. It is also immaterial here, where the contracts preclude third-party system access, regardless of whether those parties access the structure or organization of Plaintiffs' data.

the Law, however, prevents Plaintiffs from meeting these contractual duties. ER0951-952 (¶ 38); ER0970 (¶ 39).

The district court rejected this argument on the theory that the Law "does not require Plaintiffs to eliminate or reduce security for their systems." ER0018. The court relied on the statute's provisions permitting a DMS provider to decline to provide access to third-party integrators if they do not comply with certain purported security standards, A.R.S. § 28-4653.A.3(b), and providing that the statute "does not prevent" parties "from discharging [their] obligations as a service provider" under federal law, *id*. § 28-4653.C.

But requiring integrators to comply with minimum standards not even dealing with API security does not cure the Law's negative effect on system security. Testimony showed that the Law will almost certainly result in *more* integrators accessing the DMSs though integration points, increasing the number of "attack vectors" that hackers can exploit. ER0309 (72:5-18). So even if integrators could be trusted to preserve DMS security, the sheer increase in the number of integrators needlessly jeopardizes data security, impairing Plaintiffs' ability to fulfill their contractual obligations. And, as Defendants' expert pointed out, an entity could be compliant with the standards under the statute but remain insecure. ER0121 (340:5-14). The district court's reliance on the Law's empty assurances is misguided.

Finally, the Law also impairs Plaintiffs' contracts with third-party vendors prohibiting those vendors from accessing Plaintiffs' interfaces, DMS software, and other intellectual property other than as explicitly permitted by those contracts, and requiring vendors to pay market-based fees for access to Plaintiffs' DMSs. ER1235-1239 (§§ 2(a)-(e), 3); ER1240-1241 (§ 5); ER1041-1043 (§§ 2.2, 2.4); ER1044-1046 (§ 2.7).

The Law impairs both of these provisions. First, it removes Plaintiffs' contracted-for authority to determine who may integrate with their DMSs and on what terms, giving that power to the dealers instead. A.R.S. § 28-4653.A.3(b). As a result, under the Law third-party vendors may access Plaintiffs' systems as permitted by dealers, even though such vendors' contracts with Plaintiffs specify that they will only access the systems as permitted by Plaintiffs. Second, the Law prevents Plaintiffs from charging more than their "direct costs incurred … in providing protected dealer data access to an authorized integrator or allowing an authorized integrator to write data to a dealer data system." *Id*. § 28-4651(5) (defining "fee"); *id*. 28-4563.A.3(a) (prohibiting DMS providers from charging a "fee" for system access).[6]

[6] The district court did not address these claims on the merits, reasoning that Plaintiffs did not explicitly allege impairment of the vendor contracts in their complaint or in their preliminary injunction motion. ER0017 (n.10). But Plaintiffs attached the third-party interface agreements as exhibits to their preliminary injunction motion (ER1040-1067, ER1233-1246), and Defendants deposed

More broadly, the district court concluded that the Law did not severely impair Plaintiffs' dealer or vendor contracts because Plaintiffs derive only a portion of their revenue through the third-party integration fees the statute forbids, and "there is no customary practice of charging authorized third-party integrators significant fees to access a dealer's protected data."[7] ER0020-21. According to the court, "[i]t therefore cannot be seriously contended that Plaintiffs were substantially induced to enter into these contracts on the basis of their profits from third-party integrators." ER0021.

But this is beside the point, for whether there is a substantial impairment does not turn on whether there was a "customary practice" to agree to a provision, whether that provision provided a significant amount of revenue, or why a party was "substantially induced to enter into these contracts." Impairment is measured by the degree to which the challenged law changed or undermined the obligations or rights to which the parties agreed, and that impairment does not necessarily depend on the long-standing nature or relative importance to a contracting party's overall revenue

---

Plaintiffs' declarants and had ample opportunity to ask witnesses about the agreements during pre-hearing discovery. Therefore, they had adequate notice of Plaintiffs' theory.

[7] The court is incorrect that Plaintiffs have no "custom" of charging "third-party *integrators*" any fees because these "integrators" access or attempt to access Plaintiffs' systems without authorization or license. ER0949-950 (¶¶ 32-34); ER0969-972 (¶¶ 35, 41-44). Plaintiffs do, however charge licensing fees to dealers, third-party *application providers*, and other legitimate entities to access the DMS, which is the basis of Plaintiffs' business model.

stream of those rights and obligations. *See Sveen*, 138 S. Ct. at 1822-23. The Law effectively grants sub-licenses to Plaintiffs' systems despite the fact that the provisions prohibiting third-party access are at the very core of their agreements.

2. The Law interferes with Plaintiffs' reasonable expectations.

To determine whether a state law interferes with a party's reasonable expectations, the court considers "whether the industry the complaining party has entered has been regulated in the past." *Energy Reserves Grp.*, 459 U.S. at 411. The district court acknowledged that there is "no history (prior to 2019) of states regulating the relationship between DMS providers and dealers." ER0023. This factor therefore favors a finding of substantial impairment.

3. Plaintiffs cannot reinstate their rights revoked by the Law.

The final question in determining whether the Law imposes a substantial impairment of contract is whether it "prevents [Plaintiffs] from safeguarding or reinstating [their] rights." *Sveen*, 138 S. Ct. at 1822. A law that permits a party to "safeguard his contractual preferences" "with only minimal effort," such as "with the stroke of a pen," does not impose a substantial impairment. *Id*. at 1823-25. A party who "could have easily and entirely escaped the law's effect [has] no right to complain of a Contracts Clause violation." *Id*. at 1825 (internal quotations omitted). The Law prevents Plaintiffs from escaping its effect by prohibiting certain contract provisions under pain of criminal penalty and providing no mechanism for

reinstating the contract rights it eliminates. A.R.S. § 28-4653.A.3.

B. This Substantial Impairment Is Not Justified By A Law Enacted Only To Benefit A Favored Group Of Commercial Actors.

"If the state regulation constitutes a substantial impairment, the State, in justification, must have a significant and legitimate public purpose behind the regulation." *Energy Reserves Grp.*, 459 U.S. at 411-12. Only "[o]nce a legitimate public purpose has been identified" will the court then examine the statute's means-end fit. *Id*. at 412; *see Ass'n of Equip. Mfrs. v. Burgum*, 932 F.3d 727, 730-31 (8th Cir. 2019) ("The State bears the burden of proof in showing a significant and legitimate purpose underlying [the challenged law]."). To satisfy this standard, "the significant and legitimate public purpose" must be on the order of "remedying … a broad and general social or economic problem." *Energy Reserves Grp.*, 459 U.S. at 411-12. This requirement "guarantees that the State is exercising its police power, rather than providing a benefit to special interests." *Id*. at 412.

1. The Law does not seek to remedy a broad and general social or economic problem.

The district court deferred to the legislature in finding that the Law serves a legitimate end (ER0019), but deference is unwarranted, and a challenged law fails this part of the test, if the law was passed "just for the advantage of some favored group." *Keystone Bituminous Coal Ass'n v. DeBenedictis*, 480 U.S. 470, 503 (1987); *see Allied Structural Steel*, 438 U.S. at 248-49 (law that "has an extremely narrow

focus … can hardly be characterized … as one enacted to protect a broad societal interest rather than a narrow class"); *Cycle Barn, Inc. v. Arctic Cat Sales, Inc.*, 701 F. Supp. 2d 1197, 1203-04 (W.D. Wash. 2010) (same); *Ross v. City of Berkeley*, 655 F. Supp. 820, 833 (N.D. Cal. 1987) (same).

The Law fails on this ground because it was not enacted to remedy "a broad and general social or economic problem"; rather, the Law exists merely to confer a benefit on a narrow group of private parties—car dealers and, by extension, third-party vendors. The Arizona legislature made no findings that the statute addressed broad economic or social concerns. Indeed, in her legislative testimony, AADA president Bobbi Sparrow focused on her parochial complaint that DMS providers charged dealers too much for access. ER1202 (14:7-16).[8] According to Sparrow, the bill's purpose was to bar "astronomical 'data taxes' that CDK and Reynolds have imposed on dealers seeking to access their own data." ER0752 (¶ 17). This underscores the point that the Law is only aimed at helping the economic interests of certain businesses.

Further, Defendants' stated reasons for the Law are baseless. At the preliminary injunction hearing, Defendants claimed that legislators intended the Law "to protect consumer data and to prevent anticompetitive behavior surrounding this

[8] Sparrow's concern does not match the district court's finding that "there is no customary practice of charging authorized third-party integrators significant fees to access a dealer's protected data." ER0020-21.

data." ER0300 (33:16-19). But the Law does neither of these things. Defendants offered no evidence that the Law enhanced data security; rather, the Law inherently *reduces* security by rendering the system more vulnerable to attack. *See supra* pp. 31-32; ER0128 (369:2-11).

Nor did the State offer any evidence that the Law serves an antitrust-related purpose. At best, the legislative history shows a single isolated remark by Sparrow, an opaque, passing reference to the fact that Reynolds was "in the federal court right now on a big lawsuit with dealers" about "collusion and antitrust on the data." ER1186 (17:15-20). But "[s]pecial-interest groups cannot establish that legislation serves a broad societal interest simply by ensuring that the record contains testimony or floor statements about a law's conceivable public benefits." *Ass'n of Equip. Mfrs.*, 932 F.3d at 733.

Thus, Sparrow's statement is insufficient to establish that the *legislature* intended the Law to remedy any market failure, much less one posing a "broad and general" problem. *Energy Reserves Grp.*, 459 U.S. at 411-12. Instead, Sparrow's statement demonstrates that the legislature sought to "provid[e] a benefit to special interests," *id.* at 412, by upending contract terms to favor one group of economic actors over another.

The district court cited no evidence for its conclusion that the Law "seems principally designed to prevent the DMS provider from monopolizing data that is

not its own to its great financial advantage." ER0020. For there is nothing in the Law's text or legislative history suggesting that the State was concerned about anybody "monopolizing data." And in any event, "the Contract Clause prohibits special-interest redistributive laws, even if the legislation might have a conceivable or incidental public purpose." *Ass'n of Equip. Mfrs.*, 932 F.3d at 732. The Clause permits impairment of contract rights to remedy only "broad and general" problems, not to rewrite contract terms in one narrow commercial sphere. *Energy Reserves Grp.*, 459 U.S. at 411-12.

The Eighth Circuit's decision in *Association of Equipment Manufacturers* is instructive. That court upheld, on Contracts Clause grounds, a preliminary injunction enjoining a North Dakota law prohibiting farm equipment manufacturers from imposing various contractual obligations on their dealers. 932 F.3d at 729. The court reiterated an earlier holding that "'level[ling] the playing field between manufacturers and dealers'" was not a legitimate public purpose under the Contracts Clause. *Id*. at 731 (internal citation omitted). The court went on to explain that statements in the legislative history "are insufficient" to demonstrate a legislative purpose and "'a state must do more than mouth the vocabulary of the public weal in order to reach safe harbor.'" *Id*. at 733 (quoting *McGrath v. R.I. Ret. Bd.*, 88 F.3d 12, 16 (1st Cir. 1996)). Because that statute had "a narrow focus: restricting the contractual rights of farm equipment manufacturers," it "primarily benefits a

particular economic actor in the farm economy—farm equipment dealers." *Id*.

For the same reasons, there is no significant and legitimate public purpose to the Law. The Law "primarily benefits a particular economic actor": car dealers. And the Law "has a narrow focus: restricting the contractual rights" of DMS providers. There are no "well-supported findings or purposes within" the Law, just a passing remark by the AADA president, "insufficient" to establish a legitimate public purpose. Because the "design and operation" of the Law is to provide an economic benefit to a narrow group of commercial actors at the expense of another group's contract rights, the Law violates the Contracts Clause.

2. Even if there were a public purpose, the Law would be unreasonable.

Even assuming *arguendo* that the Law does serve a public purpose, "the next inquiry is whether the adjustment of the rights and responsibilities of contracting parties is based upon reasonable conditions and is of a character appropriate to the public purpose justifying the legislation's adoption." *Energy Reserves Grp.*, 459 U.S at 412. The challenged law must be "both reasonable and necessary to fulfill" the public purpose. *In re Seltzer*, 104 F.3d 234, 236 (9th Cir. 1996). The level of scrutiny increases "as the severity of the impairment" does. *Energy Reserves Grp.*, 459 U.S. at 411.

The Law compels Plaintiffs to give Arizona auto dealers control over who may access Plaintiffs' computer systems, even though this means relinquishing

property rights and jeopardizing data security and system integrity. If the purpose is to protect consumer data, the challenged provisions in the Law do not serve that purpose because they are either entirely irrelevant to security or actually increase the likelihood of a security breach. If instead the purpose is to correct a malfunctioning market, the legislature never explained what market is purportedly malfunctioning, much less link any of the Law's provisions to a market correction, and no such connection is apparent in the statute's operation.

III. The Law Conflicts With The Takings Clause.

Plaintiffs are likely to succeed on their takings claim under either a *per se* or regulatory taking theory.

A. The Law Is A Per Se Taking Of Plaintiffs' Property.

The Law *per se* violates the Takings Clause of the Fifth Amendment because it requires DMS providers to allow any third party that a dealer requests to access and write data to their DMSs. The Clause provides: "[N]or shall private property be taken for public use without just compensation." U.S. Const. amend. V. These protections apply equally to personal property as to real property. *Horne v. Dep't of Agric.*, 576 U.S. 350, 358 (2015) ("Nothing in the text or history of the Takings Clause, or our precedents, suggests that the rule is any different when it comes to appropriation of personal property.").

Likewise, the Clause protects intangible property just as it does tangible property. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003-04 (1984) (trade secret protected by Takings Clause); *James v. Campbell*, 104 U.S. 356, 358 (1881) (government cannot appropriate patent right in invention "any more than it can appropriate or use without compensation land which has been patented to a private purchaser"). Put simply, the Takings Clause "protects 'private property' without any distinction between different types [of property]." *Horne*, 576 U.S. at 359-60.

In *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 426 (1982), the Court explained that a permanent physical occupation of property by government is alone "determinative" and, without regard to whether the action achieves an important public benefit or has only minimal economic impact on the owner, results in a *per se* taking. *See id*. at 434-35. That is, when the government physically takes private personal property, it effects a *per se* taking, "however minor" the physical invasion or economic injury. *Lingle v. Chevron U.S.A., Inc.*, 544 U.S. 528, 538 (2005); *see Horne*, 576 U.S. at 359-62.

The Law is a *per se* governmental taking of Plaintiffs' private property. The undisputed evidence shows that Plaintiffs' DMSs are complex pieces of technology, consisting of millions of lines of computer code and thousands of software programs. ER0943 (¶ 5), ER0959 (¶ 3); ER0962 (¶ 12). The DMSs contain numerous proprietary databases or tables designed and organized by Plaintiffs. ER0304-305

(50:3-8, 52:5-53:22); ER0251-252 (131:3-132:10). Those databases hold information provided by dealers, OEMs, and others. ER0304 (50:10-15); ER0305 (53:2-54:13); ER0944 (¶ 9); ER0961-962 (¶¶ 8-9). While the databases contain information added by other parties, Plaintiffs wrote the code that created the databases, and Plaintiffs operate (or contract for) the computer servers that house the databases. ER304 (49:22-50:15); ER0252 (132:4-23). Plaintiffs also maintain their databases, collect, organize, and enrich the data they house, and render the data in a form useful to their dealer clients. ER0308 (67:16-68:10); ER0252 (133:8-14); ER0565 (¶ 3).[9]

The Law requires Plaintiffs and other DMS providers to permit other parties to enter, use, and occupy the providers' personal property. For example, the Law directs Plaintiffs to allow a "dealer or an authorized integrator" to "access[] or shar[e] protected dealer data" on Plaintiffs' DMS. A.R.S. § 28-4653.A.3(a). Accessing the DMSs is itself an intrusion on Plaintiffs' property rights. And that access is never passive; rather, it requires use of Plaintiffs' systems to extract the data Plaintiffs have stored and organized in their databases. *See id*. § 28-4651.1 (authorized integrator is hired "to perform a specific function for a dealer" and DMS

[9] Plaintiffs also add their own proprietary data to the DMS databases. ER0304-305 (52:24-53:7); ER0253 (139:18-24).

access is "to carry out the specified function"); *id*. § 28-4653.A.3(b) (integrators are authorized to "integrat[e] into the dealer's dealer data system").

Further, under the Law, Plaintiffs have no right to choose who may access their systems because they do not get to determine who qualifies as an "authorized integrator." *Id.* § 28-4651.1. The Law therefore removes Plaintiffs' right to exclude strangers from their DMSs because it requires them to allow any party chosen by yet another party to access, and thus use, their systems.

But the Law intrudes into Plaintiffs' property rights much further still by requiring Plaintiffs to allow dealers and third-party integrators to "writ[e] data to a dealer data system." *Id*. § 28-4653.A.3(a). This intrusion is an indefinite, and possibly permanent, occupation of space in the DMSs. While the size of data is measured in bits or bytes, and databases that house the data are not tangible in the sense they can be touched or held, databases are nonetheless personal property with defined characteristics and attributes possessing finite storage capacity. Thus, data written into Plaintiffs' systems by third-party integrators under the Law takes up some of the finite space within the database and thereby occupies a portion of it. That occupation of Plaintiffs' databases is a *per se* taking.

Loretto, 458 U.S. 419, is instructive. A New York law required property owners to permit a cable television company to install cable facilities on the roof of their property, *id*. at 421, and prohibited the landlord from demanding from the cable

company more than "a one-time $1 payment," *id*. at 423-24. The Court concluded that the permanent occupation authorized by the law was a *per se* taking because it destroyed the right to possess, use, and dispose of the landlord's property. *Id*. at 435-36. The landlord "has no power to exclude the occupier from possession and use of the space," and "[t]he power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights." *Id*. at 435; *see Ruckelshaus*, 467 U.S. at 1011-12 (explaining that for intellectual property "the right to exclude others is central to the very definition of the property interest"). Indeed, "an owner suffers a special kind of injury when a *stranger* directly invades and occupies the owner's property," an injury that "is qualitatively more severe than a regulation of the *use* of property, even a regulation that imposes affirmative duties on the owner, since the owner may have no control over the timing, extent, or nature of the invasion." *Loretto*, 458 U.S. at 436.

The Law affects Plaintiffs' property rights in a manner similar to how the New York cable law affected landlords' rights. Both laws permit occupation of property by a stranger—be it a portion of a rooftop or a portion of a database. And as in *Loretto*, where the landlords had no ability to choose who may place cable boxes on their property, here the Law removes Plaintiffs' right to choose who may write data into their systems. Moreover, the New York law restricted what landlords would receive as compensation for that occupation, and the Law similarly removes

Plaintiffs' discretion to determine how much they will be paid for allowing third-party integrators to access and occupy portions of their databases. A.R.S. §§ 28-4651.5, 28-4653.A.3(a). Like the New York landlords, Plaintiffs "suffer[] [the] special kind of injury" that occurs "when a stranger directly invades and occupies the owner's property." *Loretto*, 458 U.S. at 436 (italics omitted).

The district court rejected Plaintiffs' *per se* taking theory on three grounds: (1) "Plaintiffs have cited no authority for the provision that 'occupation' of an intangible interest like their DMS can constitute a physical taking"; (2) Plaintiffs "could meet their obligations through an API and thus without 'direct access' to Plaintiffs' DMSs by third parties"; and (3) "[t]o the extent that hardware is occupied with information provided by dealers or their authorized third parties, that is one of the benefits of the bargain the dealer receives from contracting with Plaintiffs." ER0022. None of these points is correct.

First, the district court's effort to distinguish between tangible and intangible property cannot be reconciled with the Supreme Court's plain statements that the Takings Clause applies to intangible property, *Ruckelshaus*, 467 U.S. at 1003, and "protects 'private property' without any distinction between different types." *Horne*, 576 U.S. at 358. This makes sense, for there is no principled reason to apply the *per se* taking analysis only to tangible property—the property rights to possess, use, and dispose of intangible property are the same as for tangible property, and those rights

are equally invaded when the government allows strangers to occupy it. *See, e.g.*, *Brown v. Legal Found. of Wash.*, 538 U.S. 216, 235 (2003) (holding that government program assuming intangible right to interest in lawyers' trust accounts was a taking, "akin to the occupation of a small amount of rooftop space in *Loretto*").

Second, the fact that Plaintiffs could use APIs to enable third-party integrators to access and write to the DMSs is immaterial to the takings analysis. "Indirect" access is still access, and the data that third-party integrators write to (and that therefore occupies) the DMSs exists regardless of the technical means the integrators used to put it there.

Third, if Plaintiffs had contracted with dealers to allow them to select third-party integrators to access the DMSs and write data to the system without paying a "fee," that would reflect the "benefit of the bargain" and there would be no takings claim. But Plaintiffs *did not* provide such rights to dealers, and the Law removes Plaintiffs' choice whether to contract away those rights. Thus, third-party integrators who access the DMSs and write data to the systems solely due to dealer authorization under the Law are "interloper[s] with a government license" and not merely "commercial lessee[s]." *FCC v. Florida Power Corp.*, 480 U.S. 245, 252-53 (1987). That is why the Law effects a *per se* taking.

Finally, the taking is without "just compensation." U.S. Const. amend. V. The Law forbids Plaintiffs from charging anything "beyond any direct costs incurred" in

offering access or allowing an integrator to write data to a system. A.R.S. § 28-4651.5. "The Court has repeatedly held that just compensation normally is to be measured by the market value of the property at the time of the taking." *Horne,* 576 U.S. at 368-69 (internal quotation marks omitted). By restricting Plaintiffs to direct-cost recovery, the Law denies them market value for access and write-back capability and thus denies them just compensation.

B. Plaintiffs Have A Viable Regulatory Takings Claim.

The Law also effects a regulatory taking. Regulatory takings are analyzed according to the multi-factor test in *Penn Central Transportation Co. v City of New York*, which considers "the extent to which the regulation has interfered with distinct investment-backed expectations," the "economic impact of the regulation on the claimant," and "the character of the governmental action." 438 U.S. 104, 124 (1978). No single factor is dispositive. *Dodd v. Hood River Cty.*, 136 F.3d 1219, 1229 (9th Cir. 1998). By mandating open database access, the Law will have a significant economic impact on Plaintiffs, substantially interfering with their reasonable investment-backed expectations. And at its root, the Law is a pure economic transfer from a disfavored group (DMS providers) to a favored one (car dealers).

But before turning to the traditional *Penn Central* factors, the Law fails the test right out of the gate because the taking of Plaintiffs' property is not for a public purpose. The Takings Clause "presupposes that the government has acted in pursuit

of a valid public purpose." *Lingle*, 544 U.S. at 543. The Law, however, does not benefit the public. To the contrary: By mandating uncontrolled third-party access to systems that are currently locked down securely, the Law *harms* the public. *See supra* pp. 31-32. Rather, the Law exists to benefit a single, favored group—auto dealers. *See supra* pp. 36-39.

1. The Law will interfere with Plaintiffs' distinct investment-backed expectations

The Law will interfere substantially with the way Plaintiffs have long conducted business. Plaintiffs' existing contracts prohibit their dealer customers from allowing third parties to access and write data to the DMSs without express permission. *See, e.g.*, ER00945-946 (¶¶ 13-16); ER0963-964 (¶¶ 15-16); *see also supra* pp. 29-31. The Law upends those contractual terms. A.R.S. § 28-4653.A.3(a). The very design of the Law is to permanently deprive Plaintiffs of their property by granting unfettered use to unlicensed third parties.

The district court correctly recognized that Plaintiffs had reasonable investment-backed expectations because they "were not 'on notice' that they would be regulated" in this way. ER0023 (quoting *Ruckelshaus*, 467 U.S. at 1006). Indeed, neither company could have been expected to anticipate Arizona's action. *Id.* As discussed above, there is no history of states regulating the third-party access that dealers may grant to DMSs. *Cf. Energy Reserves Grp.*, 459 U.S. at 411. No further analysis is required.

But the district court erred in placing weight on what the court considered to be the minimal investment-backed expectations at issue in light of the relatively small percentage of Plaintiffs' overall profits generated by third-party integration fees. ER0024. The *Penn Central* analysis, however, exists to analyze regulatory takings that do not completely eliminate a property's value. *E.g.*, *Tahoe-Sierra Pres. Council, Inc. v. Tahoe Reg'l Planning Agency*, 535 U.S. 302, 330 (2002). There is no "automatic numerical barrier preventing compensation in cases involving a smaller percentage diminution in value." *Cienega Gardens v. United States*, 331 F.3d 1319, 1345 (Fed. Cir. 2003).

More fundamentally, the question is whether the Law deprives Plaintiffs of the ability to achieve a "fair return" on their investment in their integration services, not on their entire portfolio. *Colony Cove Props., LLC v. City of Carson*, 888 F.3d 445, 448 (9th Cir. 2018). By analogy, a law that removes Apple's ability to achieve a return on its investment in its iPad business can be a regulatory taking even if Apple's larger consumer electronics business is unaffected.

Without experiencing any prior regulation of their integration services, Plaintiffs have invested in these programs and charge integration fees to authorized users to recoup and earn a return on their investments. *See supra* pp. 16, 32, 34. By prohibiting such fees, the Law upsets their investment-backed expectations.

2. The Law will have a significant economic impact on Plaintiffs.

The Law will interfere with Plaintiffs' efforts to monetize access to their DMS property. Plaintiffs have spent (and continue to spend) significant time and money to maintain secure DMS integration services. *E.g.*, ER00962 (¶ 12) ("hundreds of millions" of dollars "and millions of man-hours"). CDK developed its Partner Program (formerly called 3PA) and Reynolds its Reynolds Certified Interfaces (RCI) program to allow third parties to integrate with their respective DMSs and write and extract data in a safe and secure manner. ER0308 (67:4-8); ER0251 (131:22-24); ER00946-948 (¶¶ 17-31); ER0964-967 (¶¶ 17-28). Each integration point that CDK develops costs from $20,000 to several hundred thousand dollars to develop, and five percent of CDK's total revenue comes from the Partner Program. ER0255 (146:16-21); ER0259 (160:13-17).

Secured data integration is a profitable part of Plaintiffs' businesses. CDK, for instance, realizes a 36 percent profit on the Partner Program. ER0259 (161:10-14). That entire profit will be wiped out by operation of the Law, which bars DMS providers from charging anything beyond the direct costs of integration. A.R.S. § 28-4653.A.3(a). The Law will, in fact, prevent Plaintiffs from receiving *any* profit on their substantial investments in third-party integration programs.

The economic harm occasioned by the Law is not, then, a "speculative possibility," *Laurel Park Cmty. LLC v. City of Tumwater*, 698 F.3d 1180, 1190 (9th

Cir. 2012), or one founded on some "starry eyed hope of winning the jackpot," *Guggenheim v. City of Goleta*, 638 F.3d 1111, 1120 (9th Cir. 2010) (en banc). There is at least the same "reasonable probability" that Plaintiffs will continue to make these profits absent the Law as there is in "expecting rent to be paid." *Id.*

As discussed, the Law does not adequately compensate Plaintiffs for their lost integration-services profits. At best, it allows them to recover only "direct costs" occasioned by the open access that Plaintiffs must afford hostile integrators. A.R.S. §§ 28-4651.5, 28-4653.A.3(a). The market value of Plaintiffs' DMS integration services is the negotiated market rate that Plaintiffs would receive in exchange for the right to use the DMS. *See, e.g.*, *Suitum v. Tahoe Reg'l Planning Agency*, 520 U.S. 725, 741-42 (1997) ("[o]f course" the "very best evidence" of a property's market value is the "actual selling price"). The Law strips Plaintiffs of that value.

3. The Law does not merely adjust the benefits and burdens of economic life to promote the common good.

Under *Penn Central*, the Law is more akin to "a physical invasion by government" than a program "adjusting the benefits and burdens of economic life to promote the common good." 438 U.S. at 124. "[T]his is not a case in which the burden for remedying a societal problem has been imposed on all of society," *Cienega Gardens*, 331 F.3d at 1340, like the classic example of imposing prospective rent control to further the public's interest in ensuring a supply of affordable housing, *see, e.g., Guggenheim*, 638 F.3d at 1120-22. Instead, the Law

singles out a discrete population for deprivation of their property rights by another discrete population. It allows third parties to access and add data to the DMSs regardless of whether Plaintiffs would authorize that access. *See supra* pp. 42-44. It is thus closer to a "physical invasion of property" than simply an "adjustment of the benefits and burdens of economic life to promote the common good." *MHC Fin. Ltd. P'ship v. City of San Rafael*, 714 F.3d 1118, 1128 (9th Cir. 2013).

The result is no different just because the property at issue is Plaintiffs' intellectual property rather than the physical property on which their offices sit. *See supra* p. 41. As with land, "the right to exclude others is central to the very definition" of Plaintiffs' intellectual property. *Ruckleshaus*, 467 U.S. at 1011.

Finally, relevant to determining the character of the government action, the Law also imposes a direct legal obligation on Plaintiffs and is coercive, threatening criminal sanctions for failure to comply. *See, e.g.*, *Taylor v. United States*, 959 F.3d 1081, 1089 (Fed. Cir. 2020).

IV. The Law Is Void For Vagueness.

The district court dismissed Plaintiffs' claim that the Law is unconstitutionally vague under the Due Process Clause, on the grounds that "[t]he Dealer Law gives the person of ordinary intelligence a reasonable opportunity to know what is prohibited." ER0040 (internal quotations and citations omitted). But the district court erred in finding that a "person of ordinary intelligence" could reasonably

understand what conduct is prohibited under the Law's unconstitutionally vague and internally contradictory provisions. Moreover, the complaint plausibly alleges facts sufficient to support a vagueness claim, and the district court erred in dismissing the claim as a matter of law. *See* ER1156-1159. Although the Law provides no reasonable opportunity for Plaintiffs to discern its requirements or determine what actions Plaintiffs must take to comply with it, any violation of the Law could potentially expose Plaintiffs to criminal penalties, including fines of over $16,000 per day. ER1123 (¶ 21).

Any law must be "directed with reasonable specificity toward the conduct to be prohibited." *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971); *see Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926). And a statute carrying criminal penalties—as the Law does—is subject to heightened scrutiny and is unconstitutionally vague if it "fails to give ordinary people fair notice of the conduct it punishes, or [is] so standardless that it invites arbitrary enforcement." *Johnson v. U.S.*, 576 U.S. 591, 595 (2015); *see also Guerrero v. Whitaker*, 908 F.3d 541, 544 (9th Cir. 2018).

Plaintiffs challenged the Law as unconstitutionally vague because it (1) fails to put them on notice of the steps they must take to comply; (2) offers contradictory rules on whether they may put measures in place to restrict access to their systems and, if so, what types of restrictions are permissible; and (3) empowers the state to

assess criminal penalties despite these ambiguities. ER1123 (¶ 21); ER1156–1159 (¶¶ 145–58); ER1169–1170 (¶¶ 218–25).

First, Section 28-4653.A.3 prohibits Plaintiffs from taking "*any* action … to prohibit or limit a dealer's ability to protect, store, copy, share, or use" any "data that relates to a dealer's business operations in the dealer's dealer data system." A.R.S. §§ 28-4653.A(3) (emphasis added), 28-4651(7)(c); ER1157 (¶ 148). Elsewhere in the same section, however, the Law prohibits Plaintiffs from placing an "*unreasonable* restriction on integration by an authorized integrator." A.R.S. § 28-4653.A.3(b) (emphasis added); ER1158 (¶ 152), implying that there is some set of restrictions that are permissible under the act.[10] Plaintiffs cannot give meaning to both the "unreasonable" language and the full prohibition on restricting access.

But even assuming that these inconsistent statements could be reconciled to permit some "reasonable" restrictions, as the district court presumed (ER0038-39), Plaintiffs cannot determine which restrictions would qualify as "reasonable" and which would be "unreasonable." For example, Plaintiffs control access to their DMS systems using data security best practices, including authorization and credentialing; data minimization; limitations on "write" access, automated access, and access by hostile integrators with known histories of illegal activity or failure to comply with

[10] As discussed below, "unreasonable restrictions" is itself vague and incomprehensible.

industry-recognized security best practices; and contractual and technical measures that restrict sharing of certain proprietary data. ER1125-1126 (¶ 36); ER1130-1135 (¶¶ 51-68); ER1155 (¶ 142); ER1159 (¶ 157). It is unclear which—if any—of these access restrictions are "unreasonable" under the Law, and thus whether Plaintiffs are subject to criminal fines for continuing to implement them.[11]

The district court overlooked the complaint's well-pleaded allegations in dismissing this claim. The court found that the Law's prohibition on "unreasonable" access restrictions provided sufficient guidance to the parties based on their industry experience and the Law's examples of "unreasonable" restrictions. ER0038-39. But Plaintiffs sufficiently allege that, *inter alia*, the Law leaves reasonable data vendors—including those with industry experience—at a loss over which restrictions are permissible and which are "unreasonable." ER1152 (¶ 131); ER1158 (¶ 152); ER1169 (¶ 224(e)).

Other courts have reached this same conclusion in striking down similar laws

[11] Defendants' own experts demonstrated the vagaries of this prohibition. Defendants' cybersecurity expert, Mr. Kesterson, testified that in his view, "the exact same types of controls that are already in place" in Plaintiffs' systems could all be continued under the Law. ER0194 (300:6-22); *see also* ER0188-189 (279:14-17, 281:11-18, 282:14-16); ER0193-194 (299:14-300:11, 302:18-25); ER0117-118 (325:12-22, 330:17-19); ER0120 (337:17-19). Yet Alan Andreu, another defense witness, testified to the contrary, stating that in his view Plaintiffs' current restrictions, including basic security measures like CAPTCHA logins and restrictions on automated bot access, are unreasonable. ER0122-126 (346:8-362:7); *see also* ER0124-125 (352:3-15, 357:20-358:11).

involving penalties for "unreasonable" conduct. *See, e.g.*, *Johnson*, 576 U.S. at 602-03; *Guerrero*, 908 F.3d at 544. Indeed, other circuits have held that a statute using the term "reasonable" in a definition, specifically, offers insufficient guidance. For example, in *Belle Maer Harbor v. Charter Twp. of Harrison*, 170 F.3d 553 (6th Cir. 1999), the court considered a criminal statute defining a prohibited area as within a "reasonable radius." *Id*. at 555. The court found that no "commonly accepted meaning exists for the term 'reasonable' which would provide … guidance in interpreting the Ordinance and … any uniformity." *Id.* at 558. Relying on *Black's Law Dictionary*, the court noted that using a standard based in reasonableness would be susceptible to "a myriad of interpretations." *Id.*

While it may be true that a statute need not be "prolix" to pass constitutional muster (ER0038), the court erred in giving any weight to the supposed examples of unreasonableness provided in the Law. Indeed, these examples are tautological, circular, and self-referential. The Law provides six examples of "unreasonable restrictions," four of which use the word *unreasonable*. Worse, three of the four refer to "unreasonable limitations or conditions," and the ordinary understanding of the words "restriction," "limitation," and "condition" renders them synonymous with "restriction," meaning the examples define "an unreasonable restriction" as "an unreasonable restriction."

Defining unreasonableness as unreasonableness is unhelpful to a commercial party like Plaintiffs (or even Defendants) trying to understand and comply with the law, and leaves imposition of the Law's substantial criminal fines to the caprice of the enforcing official. Defendants' expert Hoyt Kesterson said it best: "I leave it to the man to my left [the judge] to define what reasonable is. That's what judges do." ER0120 (337:17-19). It is hard to imagine a more obvious example of a fatally vague criminal law.

The district court reached a contrary conclusion only by relying on several inapposite cases. For example, the court cited *Monarch Content Management LLC v. Arizona Department of Gaming.*, 2019 WL 7019416 (D. Ariz. Dec. 20, 2019), for the proposition that a statutory provision was not unconstitutionally vague where it referred to charging an "excessive or unreasonable rate." ER0039. But unlike the ill-defined standards at issue here, an excessive or unreasonable *rate* can be measured by reference to a customary rate, or some other standard. Indeed, the statute in *Monarch* incorporated a direct command to consider "prevailing rates." *Id*. at *7. Here, no such reference point exists, because the restriction does not lend itself to such a standard. It is inherently amorphous, and thus unconstitutionally vague. And whereas any misapplication of an "excessive or unreasonable rate" in *Monarch* resulted in denial of a proposed simulcast agreement, here an enforcing official's discretion as to what constitutes an "unreasonable" restriction under the Law

subjects DMS providers to significant criminal fines. *Id.*; *see also Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498–99 (1982) ("The Court has also expressed greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe.").

The court's reliance on *American Coal Co. v. Federal Mine Safety & Health Review Commission*, 796 F.3d 18 (D.C. Cir. 2015), for its conclusion that the terms "reasonable" and "unreasonable" may be "adequately specific when the parties subject to the regulation were experienced in the industry" is similarly at odds with the allegations in Plaintiffs' complaint. ER0038. *American Coal* addressed an agency interpretation of the term "fire" for purposes of safety inspections to include smoldering combustion at "reasonable" risk of igniting. 796 F.3d at 22. The court raised the importance of industry experience where both those subject to the regulation *and* those responsible for enforcing it were industry participants: "We are confident that reasonable mine operators and reasonable safety inspectors will prove able to implement the Secretary's standard in practice." *Id.* at 28. That is not the case here, where the officials tasked with enforcing the Law have little to no experience in examining the complex operations of Plaintiffs' DMS systems to determine whether and when certain access restrictions are "unreasonable," and disagreements between even Defendants' own witnesses highlight the inherent ambiguity of the statute.

The district court's effort to distinguish *St. Mark Roman Catholic Parish Phoenix v. City of Phoenix*, 2010 WL 11519169 (D. Ariz. March 3, 2010), also falls short. The court reasoned that the Law offers more objective standards than the law in that case. But the opposite is true. In *St. Mark*, there were not only multiple descriptive terms, like "unreasonably loud," "disturbing," and "unnecessary" related to a noise ordinance, but an actual decibel requirement. *Id.* at *8. Yet the vagueness claim in that case still survived a motion to dismiss.

Similarly, the district court's determination that Section 28-4651.5 sufficiently defines an impermissible "fee" as "a charge for allowing access to protected dealer data beyond any direct costs" does not address Plaintiffs' allegations that the term "direct cost" is itself ambiguous. ER0038. Considering all of the costs required for Plaintiffs merely to maintain systems capable of interfacing with authorized integrators, there is no obvious place for Plaintiffs to draw the line between "direct" costs (which may be charged) and any higher charge (which constitutes a criminal fee).

The Supreme Court has recognized "the impossibility of ascertaining" the meaning of terms that, like "direct costs," require "various factors to be considered" and are "composed of a multitude of gradations" influenced by subjective interpretation. *Connall*y, 269 U.S. at 394. The calculation and categorization of costs is particularly difficult in the software industry, where significant development

expenditure is required before launching a technologically feasible product, and there are ongoing costs to maintain and enhance existing products. *See, e.g.*, Robert F. Reilly, When Assessing Computer Software, Fair Market Value Does Not Equal Net Book Value, 23-MAR J. Multistate Tax'n 6, 10, 2013 WL 1901315 at *4 (Mar./Apr. 2013); Ryan P. Bouray, CPA, and Glenn E. Richards, CPA, Accounting for external-use software development costs in an agile environment, J. OF ACCT. (Mar. 12, 2018), https://www.journalofaccountancy.com/news/2018/mar/accounting-for-external-use-software-development-costs-201818259.html. Setting an appropriate fee, without legislative guidance, is a roll of the dice for DMS providers. ER1157-1158 (¶¶149-151). Here, as in *Connally*, "[t]he constitutional guaranty of due process cannot be allowed to rest upon a support so equivocal." 269 U.S. at 395.

Because Plaintiffs stated a valid vagueness claim under the Due Process Clause, the dismissal of the claim should be set aside.

CONCLUSION

For these reasons, the district court's order denying Plaintiffs' motion for preliminary injunction should be vacated and the matter remanded to the district court for further proceedings on that motion. Further, the district court's order dismissing Plaintiffs' CFFA preemption and vagueness claims should be reversed.

STATEMENT OF RELATED CASES

Appellants are not aware of any cases pending in this Court that are deemed related pursuant to Ninth Circuit Rule 28-2.6 or Federal Rule of Appellate Procedure 28.

RESPECTFULLY submitted this 27th day of August, 2020.

QUARLES & BRADY LLP
Renaissance One
Two North Central Avenue
Phoenix, AZ 85004

By: */s/ Brian A. Howie*
Brian A. Howie
Lauren Elliott Stine

Attorneys for Appellants

Thomas J. Dillickrath
Jonathan R. DeFosse
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
2099 Pennsylvania Ave., NW
Suite 100
Washington, DC 20006

Molly C. Lorenzi
Four Embarcadero Center, 17th Floor
San Francisco, CA 94111

Aundrea K. Gulley
Brice A. Wilkinson
Denise Drake
GIBBS & BRUNNS LLP
1100 Louisiana, Suite 5300
Houston, TX 77002

Attorneys for Appellant
The Reynolds and Reynolds Company

Britt M. Miller
Michael A. Scodro
Brett E. Legner
MAYER BROWN LLP
71 S. Wacker Dr.
Chicago, IL 60606

Mark W. Ryan
1999 K Street, NW
Washington, DC 20006

Attorneys for Appellant
CDK Global, LLC

CERTIFICATE OF SERVICE

I hereby certify that on August 27, 2020, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: August 27, 2020.

QUARLES & BRADY LLP
Renaissance One
Two North Central Avenue
Phoenix, AZ 85004

By: */s/ Brian A. Howie*
Brian A. Howie
Lauren Elliott Stine
Attorneys for Appellants

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the type-volume limitation of Ninth Circuit Rule 32-1 because this brief contains 13,993 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Microsoft Word 2013, Times New Roman 14-point font.

Date: August 27, 2020.

QUARLES & BRADY LLP
Renaissance One
Two North Central Avenue
Phoenix, AZ 85004

By:*/s/ Brian A. Howie*
Brian A. Howie
Lauren Elliott Stine
Attorneys for Appellants