UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS, in her official capacity, Defendant.	CIVIL ACTION NO. 1:20-cv-12090-DPW

DEFENDANT ATTORNEY GENERAL MAURA HEALEY'S POST-EVIDENCE MEMORANDUM

MAURA HEALEY
ATTORNEY GENERAL

Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Julia Kobick, BBO No. 680194
Assistant Attorneys General
Christine Fimognari, BBO No. 703410
Special Assistant Attorney General
One Ashburton Place
Boston, Massachusetts 02108

June 23, 2021

CONTENTS

The plaintiff Alliance for Automotive Innovation's ("Alliance"), has asserted facial, pre-enforcement claims that the Data Access Law is preempted due to conflicts with the federal Motor Vehicle Safety Act ("MVSA") and the Clean Air Act ("CAA"). In reviewing the trial evidence, it is important to remain mindful that the ultimate question is not whether certain members of the Alliance such as GM or FCA can immediately comply with the Data Access Law, but rather whether it is "a physical impossibility" for *all* OEMs to comply with both federal law and the Data Access Law, *Arizona v. United States*, 567 U.S. 387, 399 (2012), or whether the Data Access Law stands as an "'obstacle' to the accomplishment" of a "significant" objective of the federal statutes, *Williamson v. Mazda Motor of Am., Inc.*, 562 U.S. 323, 330 (2011). As the Attorney General has previously argued, the Alliance's claims fail as a matter of law because: (1) the Alliance does not have a right of action entitling it to pursue claims of conflict preemption under either the MVSA or the CAA; (2) the federal law invoked by the Alliance lacks preemptive effect; and (3) the Alliance lacks associational standing to pursue its claims.

Temporarily looking past those legal deficiencies in the Alliance's claims, this memorandum discusses the many ways in which the trial evidence demonstrated that there are multiple paths for General Motors (GM) and Fiat Chrysler Automobiles (FCA) to comply with Sections 2 and 3 of the Data Access Law that are harmonious with federal law, see pp. 2-18 below, and that, in view of the different approaches taken by different automobile manufacturers ("OEMs") to cybersecurity and to compliance with the Data Access Law, the Alliance lacks associational standing to pursue its claims, see pp. 18-20 below. This memorandum also demonstrates that nothing in the United States' Statement of Interest counsels in favor of granting relief to the Alliance. See pp. 20-22 below. Accordingly, the Alliance's request for relief should be denied, and judgment should enter in the Attorney General's favor.

I. THE TRIAL EVIDENCE HAS SHOWN THAT FCA AND GM CAN SAFELY IMPLEMENT THE DATA ACCESS LAW.

A. The Attorney General Has Proffered Reasonable Interpretations of the Law.

In evaluating a facial challenge of the type asserted by the Alliance, this Court is "required" to "consider any limiting construction that a state court or enforcement agency has proffered." *Nat'l Org. for Marriage v. McKee*, 649 F.3d 34, 66 (1st Cir. 2011) (quoting *Vill. of Hoffman Estates v. Flipside, Hoffman Estates*, 455 U.S. 489, 494 n.5 (1982)). Indeed, the state's proffered interpretation is entitled to "great weight." *McGuire v. Reilly*, 386 F.3d 45, 55, 64 (1st Cir. 2004); *accord Cape Cod Collaborative v. Dir. of Dep't of Unemployment Assistance*, 91 Mass. App. Ct. 436, 441, 76 N.E.3d 265, 269 (2017) (under Mass. law, party "challenging an agency's interpretation of a statute has the burden of proving that such interpretation is unreasonable"); *March v. Mills*, 867 F.3d 46, 67 (1st Cir. 2017) (finding "no reason not to accept [the Maine Attorney General's] perfectly sensible representation about how the disruptive-intent requirement [of challenged state statute] operates"). These precepts are particularly apt here, where the Data Access Law assigns to the Attorney General responsibilities for the enforcement of, and public dissemination of information about, the Law. *See* Mass. G.L. c. 93K, §§ 2(g) (notice requirement) & 6 (enforcement).

In addition, where a statute uses a "term of art" with an established industry meaning, a court is to "assume" that the Legislature—or, in the case of a ballot initiative, the voters—"intended it to have its established [technical] meaning," absent any contrary indication. *McDermott Int'l, Inc. v. Wilander*, 498 U.S. 337, 342 (1991); *see also La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 357 (1986) (noting "the rule of construction that technical terms of art should be interpreted by reference to the trade or industry to which they apply"); *Van Buren v. United States*, 593 U.S. --- (Jun. 3, 2021) (slip op. at 11) (courts must "take note of terms that

carry technical meaning[s]," including "when interpreting a statute about computers"). And statutory language must not be construed so as to produce an absurd result or one "manifestly at odds with the statute's intended effect." *Arnold v. United Parcel Service, Inc.*, 136 F.3d 854, 858 (1st Cir. 1998) (quoting *Parisi by Cooney v. Chater*, 69 F.3d 614, 617 (1st Cir. 1995)).

1. The Attorney General has proffered a reasonable interpretation of § 2.

Section 2 of the Data Access Law provides that:

> motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless that authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.

G.L. c. 93K, § 2(d)(1). The Attorney General has proffered interpretations of several key terms that appear in Section 2.

- The Attorney General interprets "**authorization**" to refer to an actor's role, or what the actor is and is not permitted to do on a system. Smith Aff. ¶ 182; CL ¶¶ 41-43.[1] Authorization is distinct from authentication, which refers to the confirmation of the identity of an individual, user, or other actor. Smith Aff. ¶¶ 181-83; *see also* Bort Aff. ¶ 53 (recognizing distinction); [redacted]
- The Attorney General interprets the phrase "**access to vehicle networks and their on-board diagnostic systems**" to refer only to access for obtaining data related to the purposes of diagnosis, repair, and maintenance—not open-ended access for any purpose

[1] This memorandum cites a given witness's direct testimony as "[witness last name] Aff. ¶ [paragraph number]"; a given trial exhibit as "Tr. Exh. [exhibit number]"; the transcript of the three-day evidence portion of the trial as "Tr. [trial day]:[page(s)]"; and the Attorney General's Proposed Substitute Conclusions of Law (ECF #174) as "CL ¶ [paragraph number]".

whatsoever. Tr. Exh. 30 at 3; *accord* Tr. II:65-67 (Lowe: intent of Law was to require access to vehicle networks only to the extent necessary "to get the information necessary to repair the car," and inclusion of "vehicle networks" was necessary to encompass electric vehicles, which do not necessarily have OBD systems).

- The Attorney General interprets the phrase "**entity unaffiliated with a manufacturer**" to exclude entities that have a formal corporate affiliation with an OEM or are subject to an OEM's direct or indirect control. Tr. Exh. 30 at 3-4; CL ¶ 45. The Attorney General does not interpret the phrase to prohibit *any* role by an OEM in the authorization system; to the contrary, OEMs may play a vital role in the governance model that emerges to implement the law. *Id.*; *accord* Tr. II:89 (Lowe: OEMs are "absolutely critical" in implementing the law and the governing body for the law). Similarly, the phrase "directly or indirectly" does not preclude OEMs from engaging with the repair shops, vehicle owners, or the unaffiliated entity.
- **"Motor vehicle"** is defined as any "vehicle, originally manufactured for distribution and sale in the United States, driven or drawn by mechanical power and manufactured primarily for use on public streets, roads and highways," with certain exceptions. Mass. G.L. c. 93K, § 1; *see also* Mass. G.L. c. 90, § 1. Significantly, this definition is not limited to cars powered by internal combustion engines, but rather includes electric cars.

These interpretations are reasonable, supported by evidence, and faithful to the voters' intent to assure that, "as technology advances, drivers can continue to get their cars repaired where they want." Tr. Exh. 509 at 5 (Question 1 proponents' statement in official "Information for Voters" publication); *see also*, *e.g.*, *People v. Gonzales*, 2 Cal. 5th 858, 868-70 (2017) (in interpreting

statute enacted by initiative, court "may consider the ballot summaries and arguments to determine how the voters understood the ballot measure and what they intended in enacting it").

2. The Attorney General has proffered a reasonable interpretation of § 3.

Section 3 of the Data Access Law provides that:

> [c]ommencing in model year 2022 and thereafter a manufacturer of motor vehicles sold in the Commonwealth . . . that utilizes a telematics system shall be required to equip such vehicles with an inter-operable, standardized and open access platform across all of the manufacturer's makes and models. Such platform shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. Such platform shall be directly accessible by the owner of the vehicle through a mobile-based application and, upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by [both independent mechanics and dealerships] limited to the time to complete the repair or for a period of time agreed to by the vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle. Access shall include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair.

Mass. G.L. c. 93K, § 2(f). Several key terms that appear in Section 3 are defined by Chapter 93K. Specifically:

- **"Telematics system"** is defined as "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information, in this chapter referred to as 'telematics system data,' utilizing wireless communications to a remote receiving point where it is stored." Mass. G.L. c. 93K, § 1.
- **"Mechanical data"** refers to "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle." *Id*. Mechanical data thus includes the vehicle's pre-defined diagnostic functions and any data generated, stored, or

transmitted by the vehicle and used for vehicle diagnostics, maintenance, or repair.[2] Consistent with the statutory definition, the Attorney General does not interpret this term to include any data *unrelated* to diagnostics, maintenance, or repair. *See* CL ¶¶ 36-38.

The Attorney General has also interpreted several key terms that appear in Section 3.

- The Attorney General interprets the term "**platform**" to refer to the vehicle architecture and associated software and features. Smith Aff. ¶ 112.
- The Attorney General interprets the adjective "**interoperable**" to mean a standard way to connect and communicate with the vehicle. *Id.* ¶ 113; Tr. Exh. 30 at 7. An interoperable device is one that can be used regardless of the manufacturer. Smith Aff. ¶ 113.
- The Attorney General interprets the adjective "**standardized**" to mean that which follows a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating. *Id.* ¶ 114.
- The Attorney General interprets the adjective "**open access**" to mean to have a non-gated way to gain access to the data and capabilities. *Id.* ¶ 115; Tr. Exh. 30 at 7. Open access requires the platform and the mechanical data it communicates with to be freely accessible to the owner, without the OEM acting as a gatekeeper. Smith Aff. ¶ 117. An open access platform provides a common method for any company to participate in diagnosis, maintenance, and repairs. *Id.* ¶ 116. An open access platform can still use security controls to ensure the safety and privacy of the consumer. *Id.*

[2] The trial evidence has shown that there already exists a language—the UDS protocol—used by OEMs for data related to diagnostics, repair, and maintenance that could be referenced for purposes of compliance with Section 3. Smith Aff. ¶¶ 46, 125, 127-28, 146-48, 195; [redacted].

- The Attorney General interprets the phrase "**directly accessible**" to mean that the consumer will not need to go through the OEM to perform diagnosis, maintenance, and repairs. *See* Smith Aff. ¶ 118. The consumer will only need to confirm he is the one intending to perform the diagnostics, maintenance, or repair. *Id.*
- The Attorney General interprets the phrase "**securely communicat[e]**" to mean communication in a way that authenticates the identities of the recipient and the sender, where the communication is not made known to parties other than the recipient and the sender and the integrity of the communication is not compromised. Tr. Exh. 29 at 10; CL ¶ 53.
- The Attorney General interprets the phrase "**ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair**" to mean the ability to write diagnostic data to vehicle ECUs, and to transmit packets to the ECU, if necessary for the maintenance, diagnosis, or repair of a vehicle. Tr. Exh. 30 at 7; CL ¶ 52.

Like the Attorney General's interpretations of terms in Section 2, these interpretations are reasonable, supported by evidence, faithful to the voters' intent, and ought to be credited by the Court.

B. The Trial Evidence Confirms that the Alliance's Preemption Claims Rest on Unreasonable Interpretations of the Law that Do Not Hold Up Under Scrutiny.

The evidence presented during the parties' respective cases-in-chief revealed a wide gulf between their respective interpretations of the Data Access Law. Specifically, it revealed the extremely broad interpretations of the Data Access Law relied upon by the Alliance. For example, prior to the expert "hot tub," the Alliance's expert Bryson Bort testified [redacted]

[redacted] Tr. I:187-88. Bort similarly testified that [redacted] *Id*. at 189. And he testified that he interpreted Section 2 to signify that an OEM could not affect a stranger's ability to load data onto the vehicle, and could not test such data before it was loaded.[3] Bort Aff. ¶ 59. Each of those interpretations is at odds with the Attorney General's interpretations of the Data Access Law, the multiple canons of statutory construction cited above, and the Supreme Court's admonition that state laws must be "read to avoid [preemption] concerns" whenever possible. *Arizona v. United States*, 567 U.S. 387, 413-15 (2012) ("without the benefit of a definitive interpretation from the state courts, it would be inappropriate to assume [a state law] will be construed in a way that creates a conflict with federal law"). Nonetheless, even indulging these interpretations, Bort admitted that, [redacted]. Tr. I:195.

The "hot tub" conversation made clear that the Alliance's preemption claims cannot survive reasonable interpretations of the Data Access Law. For example, Bort testified that his

[3] The testimony of the Alliance's other witnesses was much the same. [redacted]

[redacted] Tr. III:68-69. He conceded that, [redacted] *id*. at 70-71, and [redacted] *Id*. at 75. He further testified that, [redacted] *Id*. at 79. The Alliance's other expert Daniel Garrie [redacted] *Id*. at 58.

C. The Trial Evidence Has Shown that § 2 of the Law Can Safely Be Implemented.

Reasonably interpreted, Section 2 offers OEMs two methods of compliance. First, an OEM will comply with Section 2 if it does "not any require authorization" to access the OBD system. Alternatively, an OEM that *does* require authorization to access the OBD system will comply if its chosen authorization mechanism is standardized across all of its makes and models sold in Massachusetts and is administered by an unaffiliated third party.

[redacted]. This evidence that some OEMs already comply with

[4] [redacted]

Section 2 without contravening federal law is sufficient to defeat the Alliance's facial preemption claim as to that section. *See Pharm. Research & Mfrs. of Am. v. Concannon*, 249 F.3d 66, 77 (1st Cir. 2001) (facial challenge requires proof that "no set of circumstances exists under which the [statute] would be valid").

The trial evidence also showed that compliance with Section 2 through the second method is readily available using either of two preexisting technologies. One such technology is a public key infrastructure ("PKI") administered by a third party. *See* Romansky Aff. ¶¶ 6, 22-32. The trial evidence showed that [redacted] Tr. I:100-01 & 119 [redacted] The other is built upon the vehicle-to-anything ("V2X") capability powered by the security credential management system ("SCMS") developed under the auspices of the U.S. Department of Transportation. Romansky Aff. ¶¶ 33-41. As attested-to by both Bort and Smith in the "hot tub" conversation, [redacted] Tr. III:76-78, 79-81. And as Romansky testified, [redacted] *Id*. at 83.

Importantly, this second method of compliance is compatible with many preexisting cybersecurity controls. Specifically, Section 2 limits only an OEM's ability to require

authorization to vehicle repair and diagnostics. It does not limit the vehicle's ability to require authorization independent of an OEM—indeed, that is precisely what Mode 27 currently does, [redacted] Potter Aff. ¶ 48; [redacted]. Nor does Section 2 limit an OEM's ability to authenticate the identity of a prospective user, a function that, both sides' experts agreed, is distinct from authorization. Smith Aff. ¶¶ 181-83; Bort Aff. ¶ 53; [redacted]

The second method of compliance would also require a third-party entity to administer the authorization system. Although the trial yielded no evidence that such a third-party entity currently exists, the evidence amply demonstrated that one can readily be created. First, the evidence showed that an effort is already underway, led by the Auto Care Association, to create such a third-party governance entity, which would "include the OEMs as key stakeholders." Lowe Aff. ¶¶ 88-89; *see also* Tr. II:88-89 (Lowe: "I can't see how this law can be properly implemented without the manufacturers being part of it."). Second, the evidence showed that PKI administration services are currently offered by any number of independent vendors. Romansky Aff. ¶¶ 42-43; Tr. II:229-30. Third, the evidence showed that [redacted]. Tr. II:165-66. And, fourth, the evidence showed that, when prompted by state-level regulation, OEMs have a history of working cooperatively amongst themselves and with other market participants to select a third party to provide independent administration services. *See* Tr. I:11-12 (Douglas noting role of Cal. legislation in "accelerat[ing]" OEMs' work with repair shops, locksmiths, and dealers to adopt SDRM under the auspices of NASTF).

D. The Trial Evidence Has Shown that § 3 of the Law Can Safely Be Implemented.

Reasonably interpreted, Section 3 also offers OEMs multiple methods of compliance. First, because Section 3 applies only to motor vehicles that "utiliz[e] a telematics system," any car sold in Massachusetts that does *not* utilize a telematics system will comply with Section 3. The evidence has shown that [redacted]. Tr. I:57-58; *id*. at 138; McKnight Depo. at 23-24. The evidence has also shown that, [redacted] Tr. I:76. Indeed, the Alliance's experts conceded that [redacted]. Tr. I:173-75 (Bort) & 241-42 (Garrie). Rather, the trial evidence showed that disabling telematics is a safe, viable, and expeditious path to immediately implement Section 3. *See* Smith Aff. ¶¶ 19, 78-110; Tr. II:136-40. This evidence necessarily defeats the Alliance's facial preemption claim as to Section 3. *See Pharm. Research & Mfrs. of Am.*, 249 F.3d at 77.

Alternatively, if an OEM opts *not* to turn off telematics in its vehicles sold in Massachusetts, that OEM is "required to equip such vehicles with an inter-operable, standardized and open access platform across all of [that] manufacturer's makes and models." The trial evidence left no real question that, [redacted]. *See*, *e.g.*, Tr. I:56-57 ([redacted]; Tr. I:129-30 [redacted]); Tr. I:251-52 ([redacted]

[5] This is consistent with the testimony of Smith (Aff. ¶ 105) [redacted] that the removal of telematics functionality actually makes a vehicle more secure.

[redacted]); Tr. III:62-63 ([redacted] (emphasis added). Bryson Bort's testimony put it succinctly: [redacted] Tr. I:195.

To be sure, doing so would likely require modifications to internal vehicle systems. *See, e.g.*, Garrie Aff. ¶ 80 ("[R]edesigning the gateway (firewall) cybersecurity control [to comply with the Data Access Law] would require vehicle OEMs to redesign the entirety of the automobile model's cybersecurity defense, which is an expensive and time-consuming process."); Tr. I:119-20 ([redacted] *id.* at 195 [redacted] But even the Alliance's experts agreed that [redacted] Tr. I:193-95.

That GM and FCA are capable of safely implementing Section 3 should come as no surprise, because the trial evidence identified many preexisting advantages with which they would begin. For example:

- [redacted] meaning that much of the required "mechanical data" already exists in defined form. Moreover, a common diagnostic language—the UDS protocol—already is in widespread use among OEMs and would

hasten the process of creating a platform. Tr. III:55-56, 57, 79; Smith Aff. ¶¶ 46, 125, 127-28, 146-48, 195; *see also* Tr. III:68 ([redacted]).

- Both GM and FCA already utilize a robust suite of cybersecurity controls that could be re-arranged to accommodate the required platform. Those controls include "rationality" checks, the ability to authenticate firmware both upon installation and upon vehicle ignition, the use of a gateway module, the use of scan tools' Mode 27 "secure access" feature to limit access to high-risk diagnostic functions, and others.
- [redacted]. Tr. I:98, 109 (GM); Chernoby Aff. ¶¶ 48-49; McKnight Depo. at 107-08 (FCA). Indeed, [redacted]. *See* Tr. I:107-08; Tr. II:148-58; Tr. Exhs. 516, 517, 518.
- The secure vehicle interface standards ("SVI") are available to function as the standard required by Section 3. [redacted]

[redacted]

Indeed, the Attorney General's experts even proposed a medium-term solution—the use of a wireless-equipped "dongle" plugged in to the J-1962 connector—to help the OEMs comply while they develop a more permanent solution. This "dongle" solution is readily available, *see* Smith Aff. ¶ 121 (could be implemented in 6-12 months); secure, *see* Tr. II:142-45 & 161-65; and aided by the extensive preexisting use of mature telematic dongles for applications such as fleet management and diagnostics, *see* Smith Aff. ¶ 131; Potter Aff. ¶ 62; Tr. II:140, 143, & 164-65; Tr. III:65-66.

E. If the Court Concludes that Safe Implementation of the Law Will Require "Lead Time," It May Craft an Equitable Remedy that Provides Relief Limited to that "Lead Time" Period.

As discussed, the trial evidence refutes the claim by GM and FCA that the only way to satisfy the Data Access Law would be to strip cybersecurity protections from their vehicles. The trial evidence also offers insight into the real reasons for these OEMs' intransigence. Specifically, [redacted] *See* Tr. I:97 ([redacted]); Adams Depo. 79:4-21 ([redacted]); Mackay Depo. at 246 ([redacted]). [redacted] *Compare* Potter Aff. ¶¶ 47-48 (describing how most OEMs provide ETI with the permissions necessary to unlock Mode 27, which ETI's members then code onto their scan tools, "so the scan tools can access the diagnostic functions

locked behind Service 27 without having to get authorization from the manufacturer") *with* Tr. I:99-100, 106 ([redacted]); *see also* Tr. II 101-02 ([redacted]n). In addition, [redacted] Tr. I:57-58, 81-82, 241.

The trial evidence reveals that, [redacted] This is so notwithstanding this Court's admonition on January 27, 2021, that "it will be improvident of the [OEMs] not to be thinking clearly about what they're going to be doing if this initiative legislation is permitted to go into effect. . . . [T]hey better be prepared; and if they're not, that's a problem that will influence the question of preliminary injunction, I suppose, at the end." ECF #94 at 8-9.

Thus, in light of all the trial evidence, this Court should not award the Alliance any relief on its claims. Specifically, this Court should conclude that safe compliance with both Sections 2 and 3 is achievable in the near term for all of the reasons described above.

Alternatively, even if the Court were to conclude that compliance with both federal and state law is temporarily an impossibility while the platform referenced in Section 3 is being developed or while the unaffiliated entity referenced in Section 2 is being created,[6] the appropriate remedy would not be to invalidate the Data Access Law in its entirety. Rather, at most, the Court could craft an equitable remedy that (1) severs "[c]ommencing in model year 2022 and thereafter" from Section 3, and (2) enjoins enforcement of the Data Access Law for only the period of "lead time" actually needed by OEMs to comply with state and federal law.

Severability is controlled by state law. *Schwann v. FedEx Ground Package Sys., Inc.*, 813 F.3d 429, 440 (1st Cir. 2016). "Guiding this inquiry is a well-established judicial preference in favor of severability and a recognition that the [Massachusetts] Legislature has announced its own preference in favor of severability as well." *Id.* (internal quotation marks omitted) (citing Mass. G.L. c. 4, § 6). "'When a court is compelled to pass upon the constitutionality of a statute and is obliged to declare part of it unconstitutional, the court, as far as possible, will hold the remainder to be constitutional and valid, if the parts are capable of separation and are not so entwined that the Legislature could not have intended that the part otherwise valid should take effect without the invalid part.'" *Murphy v. Comm'r of the Dep't of Indus. Accidents*, 418 Mass. 165, 169, 635 N.E.2d 1180, 1183 (1994) (quoting *Mass. Wholesalers of Malt Beverages, Inc. v. Commonwealth*, 414 Mass. 411, 420, 609 N.E.2d 67, 72 (1993)).

Here, the phrase "Commencing in model year 2022 and thereafter" is logically and grammatically distinct from the substantive requirements of Section 3. And, had the voters

[6] There was evidence at trial concerning how long it might take an OEM to develop the platform: Estimates ranged from 1-2 years (Smith Aff. ¶ 209, [redacted]) to [redacted]

known that the "model year 2022" timeframe would create a compliance issue, they undeniably still would have voted for the Data Access Law's substantive requirements in view of the Law's expressed purpose to "guarantee that, as technology advances, drivers can continue to get their cars repaired where they want." Tr. Exh. 509 at 5; *see also Murphy*, 418 Mass. at 170-71 (inquiry is whether, had legislature known that particular portion of statute was unconstitutional, it would not have wanted the statute's remaining requirements); *Schwann*, 813 F.3d at 441 ("We therefore think that the legislature's plain aim in enacting this statute favors two-thirds of this loaf over no loaf at all . . . .").[7] With the "model year 2022" timeframe excised, the Court could use its equitable powers to stay the Data Access Law for the limited period of time required for OEMs to comply with the Law. *Cf. Rosie D. v. Baker*, --- F. Supp. 3d ---, No. 01-cv-30199-RGS (D. Mass. Jun. 19, 2021) (noting that "[t]he continued enforcement of an injunction . . . may well fail to account for changes in circumstances as the injunction ages" and that "'injunctions should not operate inviolate in perpetuity'") (quoting *In re Pearson*, 990 F.2d 653, 658 (1st Cir. 1993)).

II. THE TRIAL EVIDENCE HAS CONFIRMED THAT THE ALLIANCE LACKS ASSOCIATIONAL STANDING.

The evidence also confirmed that the Alliance lacks associational standing. Specifically, the evidence confirmed that "adjudicating the merits of [the Alliance's preemption claims] requires the court to engage in a 'fact-intensive-individual inquiry'" on an OEM-by-OEM basis, *N.H. Motor Transp. Ass'n v. Rowe*, 448 F.3d 66, 72 (1st Cir. 2006) (citation omitted), and thus the Alliance's claim and requested relief cannot "be adjudicated without the participation of

[7] The Massachusetts Constitution's "relatedness" requirement for initiative petitions does not alter this analysis. The purpose of this requirement—that initiative petitions contain only subjects "which are related or which are mutually dependent"—is "to avoid abuse of the process and confusion among voters" *at the time of the election*. *Anderson v. Att'y Gen.*, 479 Mass. 780, 786, 99 N.E.3d 309 (2018). It has no force after the election.

individual [OEMs] as named plaintiffs." *Me. People's Alliance & Natural Resources Def. Council v. Mallinckrodt, Inc.* 471 F.3d 277, 283 (1st Cir. 2006).

The evidence revealed that "member circumstances differ" with respect to OEMs' vehicle design and ability to comply with the Data Access Law. *Pharm. Care Mgmt. Ass'n v. Rowe*, 429 F.3d 294, 314 (1st Cir. 2005). As Smith testified, although OEMs "sometimes use common vehicle designs to try to provide a generic architecture, such designs typically support a wide number of variants, each of which may have its own characteristics. Given the diversity of vehicle architectures, there are different security considerations for each vehicle depending on how it is designed. This diversity of vehicle architectures also means that there are many different approaches that manufacturers can use to construct their vehicles to comply with" the Data Access Law. Smith Aff. ¶ 22. Bort's testimony [redacted] In particular, he explained, [redacted] Tr. I:220.

The Alliance did not provide evidence that, industry-wide, OEMs are similarly situated in their vehicle design and ability to comply with the law. The evidence was, in fact, to the contrary. For example, [redacted]. Similarly, Garrie explained [redacted]

[redacted]. *See* Tr. I:77-78, 198-99. Rather, the testimony made clear that [redacted] Tr. III:80-81. Ultimately, because the evidence demonstrated that this case necessarily involves "application of law to a series of different factual scenarios," the Alliance has not established its associational standing to represent the interests of all OEMs in this litigation. *Nat'l Ass'n of Gov't Employees v. Mulligan*, 914 F. Supp. 2d 10, 14 (D. Mass. 2012).

III. THE VIEWS EXPRESSED BY THE UNITED STATES DO NOT ALTER THESE CONCLUSIONS.

Finally, the Statement of Interest submitted by the United States lends no support to the Alliance's claims. The federal government knows how to assert preemption when it wants to do so. *See*, *e.g.*, *Arizona*, 567 U.S. at 415 ("The Federal Government has brought suit against a sovereign State to challenge the provision even before the law has gone into effect."); *Capron v. Office of Att'y Gen'l*, 944 F.3d 9, 40-44 (1st Cir. 2019) (considering, but rejecting, U.S. State Department's argument that its regulations impliedly preempt state law), *cert. denied*, 141 S. Ct. 150 (2020). Here, the United States does not contend that the Data Access Law is preempted. *See* ECF #202 at 1. It declined the Court's invitation to participate in the case, ECF #175, and it did not submit any evidence that the parties could address at trial.

Instead, the United States has merely informed the Court that, if in practice the Data Access Law "creates a safety issue constituting a defect under the Safety Act, then that Act would require motor vehicle manufacturers to recall and stop selling new vehicles compliant

with that requirement." The Attorney General does not dispute that assertion: NHTSA is authorized to order a recall when a "vehicle or equipment contains a defect related to motor vehicle safety," even if that defect is not covered by an applicable FMVSS, 49 U.S.C. § 30118(a), and the fact that an OEM might be complying with a particular state law does not limit that authority. At the same time, the fact that NHTSA can address safety risks through recalls does not warrant preemption of all state laws that touch on vehicle safety. To the contrary, MVSA's savings clause provides that NHTSA's recall authority "is in addition to other rights and remedies under other laws of the United States or a State." 49 U.S.C. § 30103(d).

As discussed, the evidence in this case has shown that an OEM such as GM or FCA can safely comply with the Data Access Law, and can do so immediately. There is therefore no basis to assume that NHTSA will ever recall any vehicle that complies with the Data Access Law, much less to find (as the Alliance's facial claim requires) that compliance will inevitably result in safety defects in all vehicles. Indeed, NHTSA admits that "the rapidly changing nature of cybersecurity safety" prevents it from "making a fact-intensive determination" whether such modifications would result in safety defects. ECF #202 at 1 n.2.

As the Data Access Law is implemented, NHTSA will remain fully able to pursue its safety mission. It can continue to update its cybersecurity "best practices" guidance to reflect its evolving understanding of those issues. It can issue guidance that is specific to the implementation of the Data Access Law in Massachusetts. Although OEMs might object, it can promulgate new FMVSS imposing binding cybersecurity requirements, which could preempt any state law that stands as an "'obstacle' to the accomplishment" of their "significant" objectives. *Williamson v. Mazda Motor of Am., Inc.*, 562 U.S. 323, 330 (2011). Or NHTSA can use its recall authority to address safety defects that actually occur.

There is therefore no basis to assume that Massachusetts officials will apply the Data Access Law "in a way that creates conflict with federal law." *Arizona*, 567 U.S. at 415. Rather, our system of cooperative federalism presumes that federal and state officials will implement overlapping administrative frameworks in a way that avoids unnecessary conflict. That principle of constitutional governance is consistent with the respect the Commonwealth has always shown for the enforcement authority of the nation's vehicle safety regulator.

CONCLUSION

For the foregoing reasons, and in view of all of the evidence and argument presented in this matter, this Court should enter judgment in favor of the Attorney General on counts 1 and 2 of the complaint.

Respectfully submitted,

ATTORNEY GENERAL
MAURA HEALEY

By her attorneys,

June 23, 2021

/s/ Eric A. Haskell

Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Julia Kobick, BBO No. 680194
Assistant Attorneys General
Christine Fimognari, BBO No. 703410
Special Assistant Attorney General
Office of the Attorney General
One Ashburton Place
Boston, Mass. 02108
(617) 963-2589
eric.haskell@mass.gov

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the CM/ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on June 23, 2021.

/s/ Eric A. Haskell
Eric Haskell