IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. AARON FREY, ATTORNEY GENERAL OF THE STATE OF MAINE in his official capacity, Defendant.	C.A. No. _____.

COMPLAINT

Plaintiff Alliance for Automotive Innovation (Auto Innovators) brings this complaint against Defendant, the Attorney General of the State of Maine, for declaratory and injunctive relief, and alleges as follows:

INTRODUCTION

1. This action challenges the threatened and actual enforcement of 29-A M.R.S. § 1810 (the "Data Law"). An express and critical prerequisite for compliance with the Data Law—an "independent entity" to develop and administer data access to vehicles—does not exist. Because compliance with the Data Law is impossible and the Data Law is unconstitutionally vague, the Data Law violates due process and harms vehicle manufacturers. Moreover, any means of compliance with the law that does not ensure cybersecurity, including any compliance strategies without the establishment of the "independent entity," is preempted by federal law.

2. The nation's leading car and light truck manufacturers—the members of Auto Innovators—take seriously their role as careful stewards of sensitive vehicle data. Each member

recognizes that unauthorized access to that data, and to the secured vehicle systems that generate that data, could, in the wrong hands, spell disaster.

3. To that end, vehicle manufacturers have developed and implemented hardware- and software-based security measures in their vehicles to ensure the integrity of their vehicle systems and the data contained on them. These security measures are intended to ensure that, *inter alia*, nefarious actors cannot remotely access or alter vehicle systems and data that control safety-critical functions, such as acceleration, braking, steering, and airbag deployment. However, access to vehicle systems and the accompanying security for that access is not subject to any particular or precise standard currently existing, and generally is administered by vehicle manufacturers themselves.

4. Despite the risks of providing external access to vehicle data, subsection 6 of Maine's new Data Law ("Subsection 6") states that, beginning no later than January 5, 2025, vehicle manufacturers must provide access "through a mobile-based application" to an "inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models." 29-A M.R.S. § 1810(6). The Data Law states this "platform must be capable of *securely* communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform." *Id.* (emphasis added).

5. Subsection 2 of the Data Law ("Subsection 2") requires that the Defendant, the Attorney General of the State of Maine, "designate an independent entity . . . to establish and administer access to vehicle-generated data . . . that is transmitted by [that] standardized access platform . . . ." *Id.* § 1810(2). The Data Law mandates that such entity "shall manage cyber-secure access to motor vehicle-generated data, including by ensuring on an ongoing basis that access to the . . . standardized access platform is secure" based on U.S. and international standards. *Id.* The

Data Law further mandates that such entity must, *inter alia*, adopt relevant standards and create policies for compliance with laws, regulations, standards, technologies, and best practices related to the access of motor vehicle data. *Id.*

6. Similarly, subsection 1 of the Data Law ("Subsection 1") mandates that access to vehicles' on-board diagnostic ("OBD") systems "may not require authorization by the manufacturer, directly or indirectly," unless that authorization "is administered by the independent entity described in [S]ubsection 2." *Id.* § 1810(1). The Data Law does not permit any other form of "authorization" for access to OBD systems.

7. Thus, for Auto Innovators' members to even attempt to comply with the Data Law's "access" requirements, or to authorize only legitimate actors to access OBD systems, several steps must have occurred: (a) the Attorney General must have designated the relevant "independent entity"; (b) that independent entity must have established and begun to administer access to vehicles through the "standardized access" platform that the Data Law contemplates, having adopted standards and policies to ensure that such access would be consistent with laws, regulations, standards, and best practices regarding access for motor vehicle data; and (c) Auto Innovators' members must have had the opportunity to implement that "standardized access" platform in their vehicles.

8. None of these steps has occurred—not even the Attorney General's designation of the independent entity that is the precursor to establishment of the "standardized access" platform that the Data Law contemplates. Accordingly, Auto Innovators' members have no ability even to start to comply with the Data Law.

9. Though they have no means of complying with the Data Law, vehicle manufacturers' purported failure to comply would subject them to substantial fines, amounting to

$10,000 per violation—several times the manufacturers' profit margin on a given vehicle. Moreover, a violation of the Data Law can constitute criminal liability, as such violations constitute Class E crimes that are punishable by up to $500 per violation, imprisonment of not more than 30 days, or both.

10. Further, the Attorney General recently has taken the position that the Data Law is immediately enforceable against Auto Innovators' members. In particular, the Attorney General has taken the position that the requirement for a "standardized and owner-authorized access platform" in Subsection 6 of the Data Law is effective and enforceable against Auto Innovators' members as of January 5, 2025. Given that the Attorney General has not designated the independent entity necessary to administer access to the "platform" referenced in Subsection 2 of the Data Law, his position concerning the immediate enforceability of Subsection 6 must mean, *a fortiori*, that the "platform" specified in Subsection 6 is different from the "platform" referenced in Subsection 2 of the Data Law; otherwise, compliance with Subsection 6 is rendered impossible due to the Attorney General's own inaction. Such a construction, however, would render the Data Law unconstitutionally vague because the same key but undefined term would have alternative meanings.

11. Acting on his view of the Data Law's effectiveness, the Attorney General has issued a notice to Maine dealerships stating that as of January 5, 2025, vehicles sold in Maine would need to be equipped with the "platform" that Subsection 6 mandates (but that no "independent entity" has created). The notice also stated that the platform would need to communicate data securely through a direct data connection to the platform—even though Subsection 2 states that the "independent entity" (which does not exist) must establish and administer access to that data. Thus, the foundational premise of that notice does not yet exist. Nevertheless, the Attorney General has

mandated that dealers must deliver that notice to prospective owners of motor vehicles, ensure that those owners have read the notice, and obtain their signature.

12. Following the Attorney General's lead, proponents of the Data Law have begun advertising to Maine residents that they should contact the Attorney General with complaints about manufacturers' purported failure to provide access to repair data under the terms of the Data Law, even though manufacturers have no ability to do so. Notably, those proponents have advocated immediate lawsuits and enforcement actions against Auto Innovators' members even though manufacturers already provide independent repair facilities with the same secure access to vehicle, maintenance, and repair data that dealerships enjoy.

13. Vehicle manufacturers cannot even begin to attempt to comply with requirements that have not yet been established by an entity that does not yet exist. Thus, the threatened enforcement of the Data Law is unconstitutional and unlawful, and/or the Data Law itself is unconstitutionally vague.

14. **First**, because compliance with Subsection 6 is impossible, holding vehicle manufacturers liable for violations of Subsection 6 would violate their due process rights. Further, if vehicle manufacturers have any obligation to comply with Subsection 6 before the creation of the relevant "independent entity" and before that entity establishes and begins to administer access to vehicles through a "standardized access" "platform" that may have different meanings across the Data Law, Subsection 6 and other provisions are hopelessly vague and fail to provide Auto Innovators' members fair notice of what they are required to do to comply with the Data Law—which also violates their due process rights.

15. Likewise, if vehicle manufacturers are required to comply with Subsection 6 before these steps occur, the Data Law directly conflicts with the requirements, purposes, and objectives

of the National Traffic and Motor Vehicle Safety Act (the "Vehicle Safety Act"), 49 U.S.C. § 30101, *et seq.*, and its regulations. If the Data Law forces vehicle manufacturers to provide an "inter-operable" and "owner-authorized access platform" before the "standardized" means of "securely communicating" data to and from that data exist, the Vehicle Safety Act and its accompanying regulations preempt that law.

16. **Second**, because the "independent entity" that is supposed to manage authorization for access to OBD systems does not exist, it is impossible for vehicle manufacturers to comply with Subsection 1 without permitting *any* person to fully access vehicles' OBD systems. Manufacturers cannot comply with Subsection 1 while ensuring that legitimate users (like vehicle repair personnel) may access OBD systems and illegitimate users (like hackers) cannot. Thus, the effect of immediate enforcement of Subsection 1 is to require manufacturers to remove vehicles' cybersecurity protections, which they cannot do consistent with their obligations under the Vehicle Safety Act and its regulations, thereby preempting immediate enforcement.

17. **Third**, the Attorney General has failed to comply with his obligations under the Data Law to designate the "independent entity" that the Data Law requires, yet simultaneously seeks to hold vehicle manufacturers liable for the consequences of not complying with the Data Law because of his failure to designate such an entity. This constitutes a "failure or refusal of an agency to act" and "refusal or failure to adopt a rule where the adoption of a rule is required by law[]" for which Auto Innovators and its members are entitled to relief pursuant to Maine's Administrative Procedures Act. 5 M.R.S. §§ 8058, 11001.

18. Accordingly, by this action, Auto Innovators seeks a declaration that compliance with the Data Law is impossible, that the Data Law is unconstitutionally vague, and that the Attorney General cannot currently enforce the Data Law. Auto Innovators further seeks an

injunction prohibiting the Attorney General from enforcing the Data Law until he has designated the relevant "independent entity," that entity has established and begun to administer access to vehicles through the "standard access" platform that the Data Law contemplates, and Auto Innovators' members have had the opportunity to implement that "standardized access" platform.

THE PARTIES

19. Plaintiff Alliance for Automotive Innovation (Auto Innovators) is a nonprofit trade association with its corporate headquarters and principal place of business in Washington, D.C. Its members include BMW of North America, LLC; FCA US, LLC; Ford Motor Co.; General Motors Co.; Honda North America, Inc.; Hyundai Motor America; Jaguar-Land Rover North America, LLC; Kia Motors America, Inc.; Mazda North America; Mercedes-Benz USA, LLC; Mitsubishi Motors of North America, Inc.; Nissan North America, Inc.; Porsche Cars North America, Inc.; Subaru of America, Inc.; Toyota Motor North America, Inc.; Volkswagen Group of America; and Volvo Cars USA.

20. Auto Innovators is the leading advocacy group for the auto industry. It was formed in 2020 from the combination of the country's two largest industry trade associations, the Alliance of Automobile Manufacturers and the Association of Global Automakers, to provide a single, unified voice for the auto industry. Auto Innovators' members are the country's leading auto manufacturers. Together, the group's members produce nearly 99 percent of the cars and light trucks sold in the United States today. Vehicles manufactured by those members are sold throughout the country, including in Maine, both through dealership sales and aftermarket used sales.

21. Defendant is the Attorney General of the State of Maine. In that position, he is the State's chief law enforcement officer, he is responsible for enforcing the Data Law, and he is

responsible for "designat[ing] an independent entity" as described in Subsection 2. The Attorney General is sued in his official capacity only.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over Auto Innovators' claims pursuant to 28 U.S.C. §§ 1331, 1367(a), and 2201(a). There is federal question jurisdiction under 28 U.S.C. § 1331 because Auto Innovators alleges violations of the federal Constitution and federal law, and the Court has supplemental jurisdiction over Auto Innovators' third cause of action under 28 U.S.C. § 1367(a). Auto Innovators, on behalf of its members, seeks a declaration of its rights pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, over which there is an actual controversy after the enactment of the Data Law and the Attorney General's actions following the enactment of the Data Law.

23. This Court has personal jurisdiction over Defendant because (a) he is located in the District in which this action was filed; and (b) many of the actions giving rise to these claims occurred in and/or were directed from this District.

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

FACTUAL ALLEGATIONS

A. Background on Motor Vehicles

25. Modern vehicles have changed a great deal since the advent of the automobile. Vehicles sold in the United States today are often as much marvels of technology as they are of mechanics. At tremendous expense, Auto Innovators' members have developed electronic systems for the vehicles in their production lineup to provide the functionality of the vehicles they sell in the increasingly high-tech new automobile market demanded by consumers.

26. But high-tech automobiles necessarily present cybersecurity challenges. As the FBI has observed, as a result of increasing Internet-connectivity, the "automotive industry will face a

wide range of cyber threats and malicious activity in the near future," with vehicles "a highly valued target for nation-state and financially motivated actors." Josh Campbell, CNN, *FBI Says Hackers Are Targeting US Auto Industry* (Nov. 20, 2019), https://www.cnn.com/2019/11/20/politics/fbi-us-auto-industry-hackers/index.html. In recent years, there have been hundreds of incidents in which hackers have targeted vehicles and the auto industry. *See, e.g.*, Jim Motavalli, Auto Week, *As Cyberattacks Ramp Up, Electric Vehicles Are Vulnerable* (Feb. 19, 2024), https://www.autoweek.com/news/a46857624/cyberattacks-on-electric-vehicles-and-chargers/; Patrick George, The Atlantic, *Car Hackers Are Out for Blood* (Sep. 11, 2023), https://www.theatlantic.com/technology/ archive/2023/09/electric-car-hacking-digital-features-cyberattacks/675284/.

27. To address this threat, Auto Innovators' members have made substantial investments to design and put in place access controls that guard the security and performance of vehicle systems, including safety-critical functions like acceleration, braking, steering, and airbag deployment. In many cases, these controls limit access to the secure parts of those systems (and the data they protect) to those authorized by the manufacturers. For instance, to conduct certain diagnostics and repairs to vehicles, it is necessary for repair personnel to send software commands to vehicle systems and/or modify the software that governs vehicle systems. To avoid nefarious actors from inappropriately altering vehicle systems and software, vehicle manufacturers limit authorization to access those features—including through such technical features as secure gateways, electronic control unit (ECU) authentication, and message authentication.

28. The development and implementation of these access and security controls are necessary to keep hackers and other unauthorized parties out of vehicle systems and to ensure the safe operation of members' vehicles in accordance with industry standards and federal law.

29. Most modern vehicles also have a telematics system that allows a vehicle to communicate remotely, enabling features such as GPS, emergency response, and remote start. Vehicle manufacturers generally separate vehicles' telematics function from other, safety-critical functions of vehicles by using secure gateways and other hardware and software features.

30. Telematics systems can also allow manufacturers to communicate recall information to consumers and deliver firmware-over-the-air updates, including to safety-related vehicle systems which allow for quicker and more comprehensive patching than traditional in-the-shop vehicle recalls. Indeed, the National Highway Traffic Safety Administration (NHTSA) strongly encourages the implementation and use of telematics systems for precisely these reasons.

B. The Data Law

31. For at least a decade, residents of Maine—like every other U.S. state—have had the ability to have their vehicles diagnosed, maintained, and repaired by repair personnel of their choice. All vehicle manufacturers who are current members of Auto Innovators agreed to a 2014 memorandum of understanding (MOU) that ensured that independent repair facilities would have a right equal to that of any dealerships to access vehicle data necessary for vehicle diagnosis, maintenance, or repair. The MOU established a dispute resolution system for access to diagnostic, repair, and maintenance data. In the decade since the MOU has been in place, no one has ever had to sue over data access or even see a dispute resolution through to completion.

32. Nevertheless, the proponents of Maine's Data Law sought and obtained its passage based upon the pretense that it would provide Maine residents with a "right to repair" their vehicles. Though framed as a "right to repair" statute, the Data Law has the effect of stripping vehicle manufacturers of their ability to secure access to the data within motor vehicles, except as established and administered by an "independent entity."

33. Specifically, Subsection 2 of the Data Law states that the Attorney General must "designate an independent entity . . . to establish and administer access to vehicle-generated data that is available through the on-board diagnostic system or that is transmitted by the ***standardized access platform*** authorized under this section," *i.e.*, the Data Law. 29-A M.R.S. § 1810(2) (emphasis added). That independent entity "must consist of one representative each from a cross section of industry trade groups including but not limited to organizations representing motor vehicle manufacturers, aftermarket parts manufacturers, aftermarket parts distributors and retailers, independent motor vehicle service providers and new car dealers." *Id.*

34. Subsection 2 further states that "[t]he independent entity shall manage cyber-secure access to motor vehicle-generated data, including ensuring on an ongoing basis that access to the on-board diagnostic system and ***standardized access platform*** is secure based on all applicable United States and international standards." *Id.* (emphasis added).

35. Lastly, Subsection 2 mandates that the "independent entity" will "[i]dentify and adopt relevant standards for implementation of [the Data Law] and relevant provisions for accreditation and certification of organizations and for a system for monitoring policy compliance;" "[m]onitor and develop policies for the evolving use and availability of data generated by the operations of motor vehicles;" and "[c]reate policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data." *Id.*

36. Two of the Data Law's other major provisions—Subsections 1 and 6—both rely upon the existence of the "independent entity" described in Subsection 2.

37. First, Subsection 1 states that "[a]ccess to the vehicle [OBD] systems of all motor vehicles . . . must be standardized and made accessible to owners and independent repair facilities

and the access may not require authorization by the manufacturer, directly or indirectly, unless that authorization is standardized across all makes and models of motor vehicles sold in this State and is ***administered by the independent entity described in [S]ubsection 2***." 29-A M.R.S. § 1810(1) (emphasis added).

38. Thus, the Data Law mandates that the Attorney General designate an independent entity that will establish and administer access to OBD systems.

39. Second, under Subsection 6, as of January 5, 2025, a manufacturer using telematics "is required to equip vehicles sold in this State with an inter-operable, ***standardized*** and owner-authorized ***access platform*** across all of the manufacturer's makes and models." 29-A M.R.S. § 1810(6) (emphasis added). "Th[at] ***platform*** must be capable of securely communicating all mechanical data[1] emanating directly from the motor vehicle via direct data connection to the ***platform***." *Id.* (emphasis added). Further, that "***platform*** must be directly accessible by the motor vehicle owner through a mobile-based application and, upon the authorization of the owner, all mechanical data must be directly accessible by an independent repair facility or a licensed dealer . . ." *Id.* (emphasis added).

40. Subsection 6 is the only portion of the Data Law (*i.e.*, Section 1810 of chapter 15 of the Maine Revised Statutes) that authorizes a standardized access platform. Indeed, other than Subsection 2, Subsection 6 is the only portion of the Data Law that even references such a "platform." Thus, the "platform" mandated and authorized in Subsection 6 is the same "platform authorized under this section [*i.e.*, section 1810]" referenced in Subsection 2. That is consistent with the original language of the ballot initiative that the Data Law's proponents presented to the

[1] "Mechanical data" is defined as "any vehicle-specific data, including telematics system data, generated by, stored in or transmitted by a motor vehicle and used in the diagnosis, repair or maintenance of a motor vehicle." 29-A M.R.S. § 1801(2-A).

Maine Secretary of State, which referred to a single "standardized access platform authorized by this law," *i.e.*, the Data Law.[2]

41. Indeed, since the passage of the Data Law, the Maine government has passed legislation acknowledging that the "platform" authorized in Subsection 6 is the "platform" referenced in Subsection 2. In particular, in April 2024, the Maine legislature passed—and Maine's Governor signed—as resolution "to Establish an Automotive Right to Repair Working Group." 2024 Me. Legis. Serv. Resolves c. 171 (S.P. 1002) (L.D. 2289). That resolution created a working group for the development of the "entity" described in the Data Law—whose responsibilities would include, among other things, "adopt[ing] standards governing access to motor vehicle telematics systems and to otherwise implement and enforce the requirements of the [Data Law]." *Id.*; *see also id.* § 2 ("The working group shall develop recommendations . . . to establish an entity to ensure cyber-secure access to motor vehicle-generated data . . . for maintenance, diagnostic and repair purposes," and those recommendations must include the development of "standards relating to access to vehicle telematics systems" and the adoption of "rules necessary for implementation and enforcement of [the Data Law] consistent with those rules.").

42. Subsection 8 of the Data Law ("Subsection 8") authorizes the Attorney General to "institute any actions or proceedings" to enforce the Data Law. 29-A M.R.S. § 1810(8). For instance, under 29-A M.R.S. § 1770, any "violation of this chapter" (*i.e.*, chapter 15 of Title 29-A of the Maine Revised Statutes, which includes the Data Law) is "a Class E crime, punishable by a fine of not less than $25 nor more than $500 or by imprisonment for not more than 30 days, or by

[2] The Secretary of State revised "this law" to "this Section," *i.e.*, section 1810, pursuant to its obligations to revise ballot initiative language for conformance with drafting conventions and the statutory numbering system, without changing the substance of the draft initiative. 21-A M.R.S. § 901(3-A).

both." Thus, the Attorney General could seek to fine or otherwise criminally penalize vehicle manufacturers who purportedly violate the Data Law.

43. Subsection 8 also authorizes "[a] motor vehicle owner or independent repair facility authorized by an owner who has been denied access to mechanical data in violation of this section" to "initiate a civil action seeking any remedies under law," including "an award of treble damages or $10,000, whichever amount is greater," for "[e]ach denial of access." 29-A M.R.S. § 1810(8).

C. Attorney General's Plan to Enforce the Data Law Despite the Non-Existence of an Independent Entity

44. Though Subsections 1 and 6 hinge upon the designation of an "independent entity" that will administer access to data transmitted through each vehicle's OBD system and "standardized access platform," the Attorney General has not designated such an independent entity. Indeed, to Auto Innovators' knowledge, no such independent entity even exists.

45. Because the Attorney General has not designated such an entity and no such entity even exists, that entity has not even begun to "establish and administer access" to data transmitted through each vehicle's OBD system and "standardized access platform." 29-A M.R.S. § 1810(2). No entity has begun to "manage cyber-secure access to motor vehicle-generated data, including ensuring on an ongoing basis that access to the [OBD] system and standardized access platform is secure based on all applicable United States and international standards." *Id.* Nor has any entity "[i]dentif[ied] and adopted relevant standards for implementation of [the Data Law]," created "policies for compliance with relevant laws, regulations, standards, technologies and best practices," or complied with any of its other obligations under the Data Law. *Id.*

46. Even if that entity existed and had undertaken those steps, vehicle manufacturers still could not comply with or implement the precise "access" (and accompanying policies and standards) established by that entity without being given significant time to do so. Vehicle

manufacturers generally "lock in" the design of a production model three to five years before it is actually released, so they have sufficient time to test and build vehicles consistent with that design. Thus, vehicle manufacturers need years of "lead time" to implement changes to their vehicles.

47. Though the Attorney General has not designated the relevant "independent entity"—which does not yet exist, much less undertaken its obligations under the Data Law—the Attorney General has taken the position that the Data Law is immediately enforceable against Auto Innovators' members.

48. The Attorney General has informed Auto Innovators of his view that the requirements set forth in Subsection 6 (which was the provision of the Data Law scheduled to take effect) are now effective, and that he may pursue purported violations of the Data Law.

49. The Attorney General has taken the position that the "platform" specified in Subsection 6 of the Data Law might be different from the "platform" referenced in Subsection 2 of the Data Law—even though Subsection 2 refers to the "platform authorized under this section" and the "platform" described in Subsection 6 is the only "platform authorized under this section."

50. Consistent with his view, on January 2, 2025, the Attorney General issued the notice to Maine automotive dealers that is attached hereto as **Exhibit A**. That notice stated that, as of January 5, 2025, vehicles sold in Maine would need to be equipped with the "platform" that Subsection 6 mandates. The Attorney General's notice to dealers included an accompanying "Maine Vehicle Telematics System Notice," which stated, among other things, that the "platform" would need to communicate data securely through a direct data connection to the platform, even though Subsection 2 states that the "independent entity" (which does not exist) must establish and administer access to that data. The Attorney General's notice to dealers mandated that they deliver the Maine Vehicle Telematics System Notice to prospective owners of motor vehicles, ensure that

those owners have read that notice, and obtain their signature—even though that notice is based upon the false premise that vehicle manufacturers have any ability to provide the "access" that the Data Law requires.

51. Following the Attorney General's lead, proponents of the Data Law have begun advertising to Maine residents that they should contact the Attorney General with complaints about manufacturers' purported failure to provide access to vehicle data under the terms of the Data Law, even though manufacturers have no ability to do so.

D. Provision of Access to OBD Systems Without Cybersecurity Protections Compromises Vehicle Safety

52. The Data Law's mandate that an "independent entity" ensure cyber-secure access to motor vehicles and that the relevant "platform" be "secure based on all applicable United States and international standards" is a recognition of the safety risks that would arise without adequately secured vehicle systems.

53. Currently, motor vehicle manufacturers perform that function. While manufacturers make some vehicle systems accessible without any authorization, they place controls and limitations on access to certain aspects of OBD-accessible systems.

54. Many modern vehicles' functions are controlled by computers and software—not mechanical functions. Thus, repairing vehicles today frequently requires repair personnel to alter vehicle software. For instance, technicians may send diagnostic commands, referred to as "writing," that cause the vehicle to execute a certain function, such as causing the car to accelerate. Technicians often must alter the software that makes vehicle components work. These include vehicle components that govern critical safety functions, such as acceleration, braking, steering, and airbag deployment.

55. In order to protect core safety functions and other vehicle components, manufacturers have developed and implemented various cybersecurity protections—such as by using challenge-and-response protocols, message authentication, encryption keys, unique identifiers for vehicle components, password protections, secure communication channels between OBD systems and offboard computer servers, secure gateways, intrusion detection and prevention systems, software authenticity and integrity checks, challenge-and-response protocols, rationality checks, secure storage controls, and firewalls.

56. Many of these cybersecurity protections are forms of "authorization" that manufacturers have imposed to protect OBD systems. For instance:

(a) *Challenge-and-response protocols.* "Challenge-and-response" protocols ensure that an appropriate person is accessing an OBD system. In a challenge-and-response protocol, when a diagnostic tool requests access to protected vehicle data or functions, a "challenge" is issued. The tool then has to give the correct "response" before the component will "unlock" the requested data or function. To give the correct response, the tool either must be programmed with a response from a manufacturer or communicate with the manufacturer's "back office," which sends the answer to the tool. This protocol, which is akin to a two-factor authentication procedure (*e.g.*, providing the answer to a "secret" question or the number sent to the user's mobile phone), ensures that only authorized users and devices are accessing vehicle systems for diagnosis, maintenance, and repair.

(b) *Message authentication.* Message authentication prevents threat actors from transmitting malware or other unauthorized communications that may affect a vehicle's core functions. Vehicle manufacturers program a vehicle's electronic control unit (ECU) to receive only messages with a secure key evidencing that the message is authorized and not malicious.

(c) *Segmentation and the secure gateway*. Vehicle manufacturers may segment vehicle systems through physical isolation (using separate processors for different functions) and logical isolation (preventing direct communication between different features). This segmentation divides the "dirty" side of the vehicle (*e.g.*, telematics systems and other functions with external connectivity) and the "clean" side of the vehicle (*e.g.*, safety-critical systems), while limiting external actors' access to the "clean" side.

(d) *Firmware encryption*. Vehicle manufacturers use asymmetric encryption techniques, termed a vehicle public key infrastructure (PKI), to secure the software that makes up an ECU. Asymmetric encryption involves both a public and private key when the firmware is installed on a vehicle. The public key allows third parties to verify that the software is authentic but still restricts access to the software, while the private key is maintained by the manufacturer on secure servers and is required to alter the firmware—thereby preventing third parties from modifying the firmware on ECUs in ways that could cause safety issues.

57. Auto Innovators' members have good reasons for maintaining these sorts of controls over access to OBD systems. Without adequate cybersecurity controls, a hacker could, for instance, cause a vehicle to accelerate without application of the accelerator pedal, or prevent the brakes from working when the vehicle exceeds a certain speed. A sophisticated hacker could even install software with delayed activation, such as disabling the brake system one month after repair is performed—making it virtually impossible to identify the malevolent actor or hold him accountable for the harm. Whatever form they take, the consequences of such an event due to compromised or non-existent access controls could be disastrous. Threats to cybersecurity are an ever-present danger today—and require constant vigilance from manufacturers to stave off.

58. It remains to be seen what the designated "independent entity" will do to ensure that access to OBD systems is sufficiently secure. However, by disregarding the mandate that an independent entity be responsible for ensuring such cyber-secure access, while simultaneously failing to designate such an entity, the Attorney General has stymied vehicle manufacturers' ability to maintain vehicle safety while complying with the Data Law.

E. The Vehicle Safety Act and NHTSA

59. The maintenance of cybersecurity controls on vehicle systems, including OBD systems, implicates the federal National Traffic and Motor Vehicle Safety Act, 49 U.S.C. § 30101, *et seq.*

60. Under the authority of the Vehicle Safety Act, the Secretary of Transportation, acting through NHTSA, acts to safeguard the public through education, research, safety standards, and enforcement.

61. NHTSA has the statutory authority to order recalls to address unreasonable risks to vehicle safety. Of the hundreds of vehicle recalls issued each year, vehicle manufacturers issue the overwhelming majority without any prompting from NHTSA. When a problem arises, NHTSA addresses safety-related concerns via direct discussions with vehicle manufacturers, often leading to manufacturers issuing a "voluntary" recall. Moreover, vehicle manufacturers have an affirmative obligation to certify compliance of their vehicles with safety standards and recall a vehicle if they become aware of a safety-related defect. Thus, the Vehicle Safety Act requires vehicle manufacturers to act regardless of whether NHTSA does so.

62. As part of its supervisory authority to promote vehicle safety, NHTSA has developed guidance to address safety problems proactively before recalls are necessary. In particular, NHTSA has advised vehicle manufacturers to implement the types of cybersecurity controls described above. As NHTSA has explained, "[v]ehicles are cyber-physical systems and

cybersecurity vulnerabilities could impact safety"—citing examples such as manipulation of vehicle sensors, braking, steering, propulsion, and power. Nat'l Highway Traffic Safety Admin., *Cybersecurity Best Practices for the Safety of Modern Vehicles*, at 1, 5, 15 (2022), *available at* https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf. Thus, NHTSA has advised vehicles manufacturer that they should:

- Limit access to vehicle ECUs' software;
- Employ "cryptographic techniques" and credentialing of users, including through passwords, PKI certificates, and encryption keys;
- Control diagnostic tools' "access to vehicle systems that can perform diagnostic operations";
- Treat "all networks and systems external to a vehicle's wireless interfaces as untrusted";
- Employ "[n]etwork segmentation and isolation techniques" and "[g]ateways with strong boundary controls";
- Employ "encryption and authentication methods in any operational communication between external servers and the vehicle"; and
- Otherwise "limit[] an attacker's ability to modify firmware."

Id. at 12-17.

FIRST CLAIM FOR RELIEF

Declaratory Judgment

(Unenforceability of Subsection 6 Due to Violation of Due Process and Federal Preemption)

63. Paragraphs 1–62 above are incorporated herein by reference.

64. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that Subsection 6 of the Data Law currently is unenforceable because it violates Auto Innovators' members' right to due process and, alternatively, it is preempted by the Vehicle Safety Act.

65. As explained, Subsection 6 requires vehicle manufacturers using telematics—including all of Auto Innovators' members—to use a "platform" created by the independent entity called for by Section 2 that allows for "**inter-operable, standardized and owner-authorized access [to mechanical data] . . . across all of the manufacturer's makes and models**." 29-A M.R.S. § 1810(6) (emphasis added). In turn, Subsection 2 describes how the "standardized . . . access platform" referenced in Subsection 6 will be created and administered by an "independent entity" designated by the Attorney General, as well as that independent entity's other responsibilities. *Id.* § 1810(2).

66. Thus, compliance with Subsection 6 requires using a "standardized access platform" in vehicles, and access through that platform must be "establish[ed] and administer[ed]" through the independent entity designated by the Attorney General. *Id.* §§ 1810(2), (6). In addition, Subsection 6 requires that access through the platform must be "secure," and it is the responsibility of the independent entity to ensure the security of the standardized access platform. *Id.* § 1810(6).

67. Providing such access currently is not possible because (a) the Attorney General has not designated an independent entity; (b) that independent entity has not established, much less started administering, the relevant access; and (c) vehicle manufacturers have not had time to adapt their vehicles to provide such access in accordance with the independent entity's instructions.

68. Because it is impossible for Auto Innovators' members to comply with Subsection 6, it would deprive them of due process to hold them liable. *See, e.g.*, *Doe v. Snyder*, 101 F. Supp. 3d 722, 724 (E.D. Mich. 2015) ("Holding an individual criminally liable for failing to comply with a duty imposed by statute, with which it is legally impossible to comply, deprives that person of his due process rights.").

69. Similarly, because the Attorney General has not designated the "independent entity" which in turn has not established or administered the relevant "access," Subsection 6 is hopelessly vague and violates Auto Innovators' members' due process rights for that additional reason. *See, e.g.*, *Frese v. Formella*, 53 F.4th 1, 6 (1st Cir. 2022) ("A statute is impermissibly vague if it 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.") (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).

70. Alternatively, to the extent the Attorney General interprets Subsection 6 to permit compliance by providing an "access platform" *without* the "cyber-secure" access that the independent entity is supposed to establish and administer, the Vehicle Safety Act and its implementing regulations preempt that interpretation.

71. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

72. A failure to maintain adequate cybersecurity controls would give rise to a safety-related defect, and the Vehicle Safety Act requires manufacturers to issue recalls and remediate

safety-related defects. Therefore, providing non-secure access would conflict with the purposes and objectives of the Vehicle Safety Act.

73. The Data Law is similar to, and largely based upon, a ballot initiative passed in Massachusetts in 2020, which is codified at Chapter 93K of the Massachusetts General Laws (the "Massachusetts Data Access Law"). NHTSA has recognized that if the Massachusetts Data Access Law's access requirements would create safety issues, then the Vehicle Safety Act would require motor vehicle manufacturers to recall and stop selling new vehicles compliant with that requirement. Thus, in June 2023, NHTSA specifically instructed Auto Innovators' members that "the [Massachusetts] Data Access Law conflicts with and therefore is preempted by the [Vehicle] Safety Act."

74. Nevertheless, as explained, the Attorney General has taken the position that the Data Law is immediately enforceable and effective and that Auto Innovators' members can be held liable under the Data Law. Therefore, an actual controversy exists between the parties regarding the enforceability and effectiveness of Subsection 6 of the Data Law.

75. Accordingly, Auto Innovators is entitled to a declaration that Subsection 6 currently is unenforceable because it violates Auto Innovators' members' right to due process or, alternatively, is preempted by federal law.[3]

[3] Auto Innovators reserves its right to advance further claims and/or arguments, including regarding preemption of the Data Law, based upon any particular interpretation of the Data Law that the Attorney General asserts, and/or the standards and regulations that the "independent entity" adopts following its creation and designation by the Attorney General.

SECOND CLAIM FOR RELIEF

Declaratory Judgment

(Unenforceability of Subsection 1 Due to Violation of Due Process and Federal Preemption)

76. Paragraphs 1–75 above are incorporated herein by reference.

77. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court's inherent equitable authority, and seeks a declaration that Subsection 1 of the Data Law currently is unenforceable because it either violates Auto Innovators' members' right to due process or is preempted by the Vehicle Safety Act.

78. As explained, Subsection 1 states that "[a]ccess to the vehicle on-board diagnostic systems of all motor vehicles . . . may not require authorization by the manufacturer, directly or indirectly, unless that authorization is standardized across all makes and models of motor vehicles sold in this State and is administered by the independent entity described in [S]ubsection 2." 29-A M.R.S. § 1810(1). In turn, Subsection 2 states that the relevant independent entity will "establish and administer access to vehicle-generated data that is available through the on-board diagnostic system . . . ." *Id.* § 1810(2).

79. Thus, manufacturers may not "require authorization" to access OBD systems unless that authorization is administered by the "independent entity" that does not yet exist. Holding manufacturers liable for imposing authorization that is not administered by that independent entity—when such entity does not exist and has not established and begun administering the relevant standards—would violate their due process rights. *E.g.*, *Snyder*, 101 F. Supp. 3d at 724; *Frese*, 53 F.4th at 6.

80. The only alternative, theoretical means of compliance under Subsection 1 is to provide access without any authorization by the manufacturer. But existing cybersecurity protections (which are not administered by the independent, third-party entity) necessarily require

manufacturers to impose limits on access to OBD systems, which encompasses the vehicle's internal system that monitors and reports vehicle performance issues. Thus, removal of that authorization would require removal of cybersecurity protections that would give rise to a safety-related defect.

81. Nevertheless, as explained, the Attorney General has taken the position that the Data Law is immediately enforceable and effective and that Auto Innovators' members can be held liable under the Data Law. Therefore, an actual controversy exists between the parties regarding the enforceability and effectiveness of Subsection 1 of the Data Law.

82. Accordingly, Auto Innovators is entitled to a declaration that Subsection 1 currently is unenforceable because it violates Auto Innovators' members' right to due process and/or is preempted by federal law.

THIRD CLAIM FOR RELIEF

Declaratory Judgment

(Relief under Maine Administrative Procedures Act for Attorney General's Failure to Designate Independent Entity)

83. Paragraphs 1–82 above are incorporated herein by reference.

84. This claim is brought under the Maine Administrative Procedure Act ("Maine APA"), 5 M.R.S. § 8001 *et seq.*; 28 U.S.C. § 1367(a); and this Court's inherent equitable authority, and seeks a declaration that Subsections 1 and 6 of the Data Law currently are unenforceable because the Attorney General has failed to designate the "independent entity" that the Data Law mandates.

85. The Maine APA permits "[a]ny person aggrieved by the failure or refusal of an agency to act" to seek "judicial review" of that failure or refusal. 5 M.R.S. § 11001. Likewise, "any person who is aggrieved" by "an agency's refusal or failure to adopt a rule where the adoption

of a rule is required by law[]" is entitled to "[j]udicial review" of that refusal or failure, and the court may "issue such orders as are necessary and appropriate to remedy such failure." *Id.* § 8058.

86. The Attorney General is an "agency" as defined in the Maine APA. *See id.* § 8002(2) ("'[a]gency' means any body of State Government authorized by law to adopt rules, to issue licenses or to take final action in adjudicatory proceedings, including, but not limited to, every . . . officer of the State Government so authorized," subject to certain exceptions not applicable here).

87. The Attorney General's designation of an "independent entity" under Subsection 2 is the adoption of a "rule" as defined in the Maine APA. *See id.* § 8002(9) ("Rule" encompasses any "regulation, standard, code, statement of policy, or other agency guideline or statement of general applicability" that "is intended to be judicially enforceable and implements, interprets or makes specific the law administered by the agency."). Alternatively, it is a final agency action. *Id.* § 8002(4).

88. The Attorney General has not designated an "independent entity" under the Data Law, which is a "failure or refusal . . . to act" and a "refusal or failure to adopt a rule" that was required by law. *Id.* §§ 8058, 11001. Nevertheless, as explained, the Attorney General has taken the position that the Data Law is immediately enforceable and effective and that Auto Innovators' members can be held liable under the Data Law. An actual controversy exists between the parties regarding the enforceability and effectiveness of the Data Law in the absence of the Attorney General's designation of the "independent entity."

89. Auto Innovators and each of its members are "person[s] . . . aggrieved" by that conduct. 5 M.R.S. §§ 8058, 11001. The Data Law specifically contemplated that vehicle manufacturers would be able to comply with the Data Law—purportedly while maintaining cyber-

secure vehicle systems—by relying upon an independent entity, designated by the Attorney General, that would include industry representatives (including organizations representing motor vehicle manufacturers) that would establish and administer access to vehicle data. As a result of the Attorney General's failure to designate an entity and the resulting failure of any entity even to begin to establish or administer data access, Auto Innovators' members face crippling financial liability from civil actions and potential criminal liability.

90. Accordingly, Auto Innovators is entitled to a declaration that Subsections 1 and 6 of the Data Law currently are unenforceable because the Attorney General has failed to designate the "independent entity" that the Data Law mandates.

FOURTH CLAIM FOR RELIEF

Injunctive Relief

91. Paragraphs 1–90 above are incorporated herein by reference.

92. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, the Maine APA, and this Court's inherent equitable authority, and seeks an injunction prohibiting enforcement of Subsections 1 and 6 until the Attorney General has designated the relevant independent entity, that independent entity has undertaken its obligations under Subsection 2, and vehicle manufacturers have had an opportunity to comply with the access requirements that the independent entity has established and administered.

93. Absent an injunction, Auto Innovators' members would face civil and criminal liability from premature enforcement of the Data Law. Further, any attempts at compliance before the relevant "independent entity" has created and begun to administer cyber-secure access to vehicle mechanical data could undermine the integrity of motor vehicle systems and the safe operation of consumer vehicles. Premature enforcement or attempts at compliance could harm manufacturers' business reputations, result in exposure to claims by customers, and/or result in the

considerable costs of conducting recalls mandated by NHTSA, which includes the mandatory "stop sale" of all vehicles containing the safety-related defects leading to the recalls.

94. Defendant and third parties would not be harmed by an injunction, which would preserve the status quo, in which Maine consumers enjoy complete mechanical data access (to the extent any such data is necessary for vehicle diagnosis, repair, and maintenance) to have their vehicles repaired at any facility they choose or to enable the repair themselves. Further, an injunction would serve the interest of the public, which has a strong interest in halting the enforcement of unconstitutional laws and state laws that directly conflict with federal law, as well as the protection of consumer safety.

PRAYER FOR RELIEF

Plaintiff respectfully requests that the Court enter judgment:

A. Declaring that Subsections 1 and 6 currently are unenforceable because they violate Auto Innovators' members' right to due process and/or are preempted by federal law;

B. Declaring the Data Law unconstitutionally vague;

C. Temporarily and permanently enjoining enforcement of Subsections 1 and 6 until the Attorney General has designated the relevant independent entity, that independent entity has undertaken its obligations under Subsection 2, and vehicle manufacturers have had an opportunity to comply with the access requirements that the independent entity has established and administered;

D. Awarding Plaintiff its costs and litigation expenses, including attorneys' fees and costs, pursuant to 42 U.S.C. § 1988; and

E. Awarding Plaintiff such other and further relief as the Court deems just, proper, and equitable.

Dated: January 31, 2025

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Joshua D. Dunlap

Joshua D. Dunlap
Shannon Linnehan
PIERCE ATWOOD LLP
254 Commercial Street
Merrill's Wharf
Portland, ME 04101
Tel: (207) 791-1100
jdunlap@pierceatwood.com
slinnehan@pierceatwood.com

John Nadolenco (*pro hac vice* pending)
Erika Z. Jones (*pro hac vice* pending)
Daniel D. Queen (*pro hac vice* pending)
Eric A. White (*pro hac vice* pending)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
jnadolenco@mayerbrown.com
ejones@mayerbrown.com
dqueen@mayerbrown.com
eawhite@mayerbrown.com

Charles H. Haake (*pro hac vice* pending)
Jessica L. Simmons (*pro hac vice* pending)
ALLIANCE FOR AUTOMOTIVE INNOVATION
1050 K Street, NW
Suite 650
Washington, DC 20001
Tel: (202) 326-5500
chaake@autosinnovate.org
jsimmons@autosinnovate.org

Exhibit A

AARON M. FREY
ATTORNEY GENERAL

TEL: (207) 626-8800
TTY USERS CALL MAINE RELAY 711

STATE OF MAINE
OFFICE OF THE ATTORNEY GENERAL
6 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0006

REGIONAL OFFICES
84 HARLOW ST. 2ND FLOOR
BANGOR, MAINE 04401
TEL: (207) 941-3070
FAX: (207) 941-3075

125 PRESUMPSCOT ST., STE. 26
PORTLAND, MAINE 04103
TEL: (207) 822-0260
FAX: (207) 822-0259

14 ACCESS HIGHWAY, STE. 1
CARIBOU, MAINE 04736
TEL: (207) 496-3792
FAX: (207) 496-3291

NOTICE TO MAINE DEALERS

Under Maine law, 29-A M.R.S.A. § 1810, vehicle owners have the right to access their vehicle's mechanical data through a mobile device and to authorize an independent repair facility to access the vehicle's mechanical data to diagnose, repair, and maintain the vehicle. As of January 5, 2025, manufacturers of motor vehicles sold in Maine, including commercial motor vehicles and heavy-duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that use a telematics system, are required to equip vehicles sold in Maine with an inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models.

As required by Maine law (29-A M.R.S.A. § 1811), the Attorney General has established for prospective motor vehicle owners the accompanying Maine Motor Vehicle Telematics System Notice. Please note that the notice form provides for the prospective motor vehicle owner's signature certifying that the prospective owner has read the telematics system notice.

DEALER OBLIGATIONS: When selling or leasing motor vehicles containing a telematics system, a dealer as defined in Title 29-A, section 851, subsection 2 and a new vehicle dealer as defined in section 851, subsection 9 shall provide the telematics system notice under subsection 1 to the prospective owner, obtain the prospective owner's signed certification that the prospective owner has read the notice and provide a copy of the signed notice to the prospective owner.

Maine Vehicle Telematics System Notice

This vehicle includes a "telematics system" as defined under Maine Revised Statutes, Title 29-A, section 1801(6). Under Maine law, you have the right to access the vehicle's mechanical data through a mobile device and to authorize an independent repair facility to access the vehicle's mechanical data to diagnose, repair, and maintain your vehicle.

A vehicle's telematics system collects information generated by the operation of the vehicle and transmits that information using wireless communications to a remote receiving point where the information is stored or used.

As of January 5, 2025, manufacturers of motor vehicles sold in Maine, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that use a telematics system, are required to equip vehicles sold in Maine with an inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models. The platform must be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. The platform must be directly accessible by the motor vehicle owner through a mobile-based application and, upon the authorization of the owner, all mechanical data must be directly accessible by an independent repair facility or a licensed dealer limited to the time to complete the repair or for a period of time agreed to by the motor vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle.

"Mechanical data" refers to vehicle-specific data, including telematics system data, generated by, stored in, or transmitted by a motor vehicle and used in the diagnosis, repair, or maintenance of the vehicle. The type of mechanical data available through telematics will vary depending on the vehicle, but can come from sensors on many vehicle parts, such as the airbags, battery, engine and/or motor, transmission, brakes, or tires.

Certification of Notice

Prospective Owner 1

I hereby certify that I have been provided with and read the Maine Vehicle Telematics System Notice on this _____ day of _____, _____.

_____ _____
Name (Printed) Signature

Prospective Owner 2

I hereby certify that I have been provided with and read the Maine Vehicle Telematics System Notice on this _____ day of _____, _____.

_____ _____
Name (Printed) Signature

_____	_____
Make	Model and Model Year
_____	_____
Seller Name	VIN
_____	
Seller Address	