IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW

Declaration of Kevin Tierney

1. My name is Kevin Tierney. I am 42 years old and reside in Brighton, Michigan.

2. Since 2019, I have been the Vice President of Global Cybersecurity at General Motors Company ("GM"), responsible for overseeing GM's global cybersecurity program. This declaration is based on my personal knowledge. I am submitting this declaration at the request of the Alliance for Automotive Innovation ("Auto Innovators"), of which GM is a member.

Introduction and Background

3. Both in my capacity as GM's Vice President of Global Cybersecurity and as a witness in this case, I have paid close attention to this action since it began in late 2020. I have become familiar with the Attorney General's position regarding the meaning and requirements of the Data Access Law, with the testimony from the president of the Auto Care Association (ACA) regarding the intentions behind the ballot initiative that led to the passage of that law, and with the Attorney General's experts' ideas about how to implement the Data Access Law. Most recently, I have reviewed the parties' joint submission regarding their respective interpretations of the Data Access Law. Having considered for months now the Attorney General's proposed solutions and

interpretations, it remains my considered judgment that it is simply impossible to comply with the Data Access Law safely—and that the proposed methods of compliance proposed by the Attorney General's experts are not viable and little more than interesting ideas that, when considered carefully, do not work.

4. One of the more confusing aspects of this case is that the Data Access Law was ostensibly intended to improve consumers' "right to repair" their motor vehicles. Having reviewed the ACA's concerns during the trial, however, that premise for the law is incorrect. If, as they claim, all they want is to be on equal footing with dealers when it comes to the data needed to repair vehicles, they are. ACA's concern that GM dealers use telematics data to repair, diagnose, or maintain vehicles proved unfounded at trial. They don't.

5. Even before the passage of the Data Access Law, Massachusetts law required that OEMs provide access to on-board diagnostic and repair information systems using a personal computer and physical interface device. Further, GM, like other OEMs, complies with the 2014 Memorandum of Understanding (MOU) between auto manufacturers' trade associations, the Coalition for Auto Repair Equality (CARE), and the Automotive Aftermarket Industry Association (AAIA), which provides that independent repair facilities across the United States have the same access as dealers to diagnosis, maintenance, and repair data. That MOU includes mechanisms for consumers or repair shops to complain about any claimed violation of the OEMs' obligations and to ultimately resolve those complaints through a dispute resolution panel (DRP). Not surprisingly given its commitment to ensuring independent access to GM vehicles' on-board diagnostic systems, it has never been necessary to convene a DRP with respect to GM vehicles. Therefore, right now, in Massachusetts—as in the rest of the United States—independent repair shops are

already able to diagnose, maintain, and repair GM vehicles on the same terms as GM's own franchise dealers.

6. For instance, GM provides data and information necessary for diagnosis, maintenance, and repair of GM vehicles through an online portal called the ACDelco Technical Delivery System (TDS). Any aftermarket service provider may subscribe to TDS and receive the same repair information and data that GM franchised dealers receive, on the same terms that those dealers enjoy. Using TDS, GM makes software repair "parts" fully available to aftermarket service providers at the same time as it makes that software available to its franchise dealers. Similarly, using TDS, GM makes its service manuals fully available to aftermarket service providers at the same time as it provides them to dealers. In addition, GM does not require the use of GM physical tools to repair GM vehicles. Rather, GM vehicles permit the use of tools manufactured by aftermarket service providers.

7. GM does not have any plans to end this consumer choice. To the contrary, GM intends to continue to make diagnostic, maintenance, and repair information and data available in future motor vehicles. GM has announced that it will sell all-electric vehicles by 2035. Notwithstanding that announcement, *GM will continue to make diagnostic, maintenance, and repair information and tools for all its vehicles, including electric vehicles, available to both independent repair shops and franchised dealers*, and it will continue to provide OBD-II ports on all of its vehicles for that purpose.

8. In fact, GM is involved in industry-wide efforts to ensure that consumers can continue to service their vehicles with whichever service provider they choose. For example, Robert Stewart, GM's Aftermarket Service Manager, is a Director and Vice Chairman of the National Automotive Service Task Force (NASTF), which facilitates communications between

automakers, independent repair technicians, and other automotive industry participants; provides resources and information to service technicians and other individuals who seek to repair motor vehicles; and manages the release of replacement keys to automotive locksmiths under the Secure Data Release Model (SDRM) program.

9. Though I understand that the ACA pursued the ballot initiative in Massachusetts to ensure access to data from GM's telematics units, that data has very little to do with the diagnosis, maintenance, or repair of vehicles. GM's telematics service, OnStar, only transmits and receives repair data to (a) provide firmware-over-the-air updates (FOTA), whereby GM provides software updates to vehicle owners, free-of-charge; and (b) send diagnostic reports with information about the status of key vehicle systems, such as airbag, antilock braking, engine, emissions, and stability control systems, if the owners choose. Neither of these services affect vehicle owners' ability to choose independent service providers to service their vehicles. Consumers can provide those diagnostic reports to any repair technician, whether that is an independent repair shop or a GM franchise dealer. Further, the limited diagnosis, maintenance, and repair information that is transmitted through GM's telematics units is a small subset of the overall data that any repair shop can access via a GM vehicle's OBD-II port.

10. In short, GM vehicle owners already have the ability to take their vehicles to any independent service provider they choose, and GM does not inhibit that choice. The effect of the Data Access Law is to impose a number of requirements that do not meaningfully expand Massachusetts voters' "right to repair," but creates untenable safety risks to GM and other vehicles that GM is simply unwilling to accept.

GM's Inability to Comply with the Data Access Law

11. With that backdrop in mind, I address the Court's inquiry about any steps taken to implement the requirements of the Data Access Law since last year's trial. The short answer is that GM cannot implement those requirements (as it understands them) at this time, and therefore has not implemented those requirements. There are several major reasons for this.

12. Preliminarily, as I explained at length in my June 10, 2021 trial affidavit, implementing the Data Access Law would require removing various cybersecurity protections that GM has placed around safety-critical vehicle functions and emissions controls that are mandated by federal law. Indeed, certain requirements of the Data Access Law—such as its requirements that access be given to "vehicle networks," that vehicles be equipped with an "open access" platform, that the platform be "directly accessible," and that this access include the ability to "send commands" to in-vehicle components—are antithetical to good cybersecurity practice. As NHTSA emphasized in its most recent cybersecurity guidance, issued just last month: "Vehicle and diagnostic tool manufacturers should control tools' access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control." NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles* (Sep. 2022) ("2022 NHTSA Cybersecurity Best Practices") § 8.4. The Data Access Law would preclude such authentication and access control. GM cannot comply with the Data Access Law for that reason alone.

13. However, even beyond cybersecurity-specific concerns, there are basic practical obstacles that prevent GM from being able to comply with the Data Access Law.

14. First, before GM can realistically begin trying to comply with the law, it needs to know exactly what the Data Access Law requires. For instance, Section 2 of the Data Access Law

requires the creation of a third party that the Attorney General says cannot be affiliated directly, indirectly, or contractually with the OEMs. That third party will control the security for accessing all vehicles in the Commonwealth. For starters, as I explained at trial, that creates an untenable and unacceptable cybersecurity risk by creating a single attack surface across all OEMs, and it is inconsistent with the diversity protocols that good cybersecurity practices require. In addition to that risk, however, that third party does not exist. The OEMs cannot themselves create an entity that is "unaffiliated" with them, and such an entity would require the input from other industry stakeholders, including other aftermarket parts businesses and independent vehicle service providers. Until such a third party does exist and creates a standardized and secure authorization system, I simply cannot even begin to design GM vehicles that comply with Section 2.

15. Additionally, while I understand that Auto Innovators and the Massachusetts Attorney General agree about the meaning of some of the provisions of the law, I understand they disagree about the meaning of other provisions and the practical requirements that the law imposes. Further, I understand that neither Auto Innovators' nor the Attorney General's interpretation of the laws have any binding effect. Therefore, GM simply needs guidance from the Court about the law's requirements before it can make any meaningful progress toward compliance.

16. Second, putting aside those uncertainties, and as discussed in more detail below, the Data Access Law imposes a number of prerequisites that do not exist and are outside of GM's control. By way of example, section 2 references "standardized" access to vehicle on-board diagnostic systems, and section 3 references a "standardized" platform, but no such standards currently exist.

17. The design and production process necessary for vehicles exacerbates these problems. GM, like other OEMs, follows a detailed and stringent product development process

that requires extensive testing for federal and state regulatory compliance, product assurance, consumer preference, cybersecurity, and product safety. It takes years to design, test, and ultimately manufacture vehicles. (For instance, GM completed the electrical architecture design for model year 2022 vehicles between April 2017 and June 2019, and it completed the validation process for those vehicles before November 2020, when the Massachusetts voters passed the ballot initiative in this case.) GM cannot embark upon this years-long development process without having certainty about the legal requirements, standards, and other features of the Data Access Law to which GM would need to conform its vehicles.

18. In sum, GM simply cannot comply with the Data Access Law. But as noted, my team and I have carefully considered the Attorney General's proposed methods for compliance before, during, and after the trial. Below, I make clear why those methods do not work.

Attorney General's Proposed Methods for Compliance

19. The Attorney General has proposed various methods for GM to attempt to comply with the Data Access Law, which are summarized at paragraphs 171 to 245 of the Attorney General's Proposed Revised Substitute Findings of Fact and Conclusions of Law ("AG PFOF"). I have reviewed those proposals with respect to GM vehicles and found that, in addition to the cybersecurity issues associated with those proposals that I described in my trial affidavit and testimony, GM cannot safely comply (or even attempt to comply) with those proposals.

Section 2: No Manufacturer Authorization

20. The Attorney General first suggests that GM can comply with Section 2 of the Data Access Law by allowing access to on-board diagnostic systems without requiring any manufacturer authorization. AG PFOF ¶ 172. The Attorney General notes that many OEMs prohibit access to diagnostic functions by using an OEM-specific key to unlock "Mode 27," which

is a mode that permits secure access to diagnostic functions in some motor vehicles. However, the Attorney General says those OEMs nonetheless can comply with Section 2 by disseminating those keys to repair tool manufacturers through the Equipment and Tool Institute (ETI), and that this is not "authorization from the manufacturer." *Id.* ¶ 173.

21. However, Section 2 of the Data Access Law states that "access to vehicle on-board diagnostic systems shall . . . not require any authorization by the manufacturer, directly or *indirectly*" (emphasis added). Therefore, to the extent OEMs' use of keys disseminated through ETI is a form of "indirect" authorization, the Attorney General's proposed solution does not work.

22. Similarly, that same portion of Section 2 states that the "access to vehicle on-board diagnostic systems" must be "standardized." However, the software that is used to diagnose, maintain, and repair GM vehicles is proprietary and unique to GM (and, in some cases, to particular vehicles) and is not "standardized." The same is true for other OEMs. No "standardized" software exists because every OEM uses one or more unique vehicle architectures with unique features.

Section 2: System of Authorization

23. The Attorney General alternatively suggests that GM can comply with Section 2 of the Data Access Law by implementing an authorization system that is "administered by an entity unaffiliated with it" and "shared among all OEMs that wish to require authorization to access vehicle on-board diagnostic systems." *Id.* ¶ 175. The Attorney General proposes designing that access using a Public Key Infrastructure (PKI) and/or Vehicle-to-Anything (V2X) technology. *Id.* ¶¶ 177, 185. I am not aware of any OEM that has been able to develop PKI and/or V2X technology for use in the manner that the Attorney General suggests. Indeed, I am not aware of any OEM that has been able to broadly deploy V2X technology. Although OEMs have been experimenting with that technology for years, their efforts to implement it have been delayed because of (among other

factors) the complexity of security that would be required for that technology. These proposals are nothing more than theoretical possibilities—not technologies that have been tried and tested to work as broad authorization systems in the context of vehicle diagnosis, maintenance, and repair.

24. The Attorney General's proposed solutions also do not appear to explain how the relevant authorization systems would provide access to "vehicle networks" in addition to on-board diagnostic systems. To the extent that Section 2 requires access to both "vehicle networks and their on-board diagnostic systems," the Attorney General's proposed solutions do not work.

25. Perhaps more importantly, this portion of the Data Access Law requires that the relevant authorization system be "standardized across all makes and models sold in the Commonwealth" and "administered by an entity unaffiliated with a manufacturer." Again, this creates unacceptable cybersecurity risks. Further, there is no "standardized" authorization system that currently exists, and development of such a system would require the input of aftermarket representatives, including tool developers and independent repair providers. Likewise, there is no "entity unaffiliated with a manufacturer" that exists to implement this authorization system, and OEMs cannot themselves create an entity that is "unaffiliated" with them.

26. The Attorney General suggests that such an "unaffiliated entity can readily be created." *Id.* ¶ 192. That is a vast overstatement that ignores reality. First of all, it is entirely unclear in the Massachusetts law who is going to create this entity, but it certainly is not the OEMs, as they cannot be affiliated with that entity. To create an independent body that provides "standardized" access to all manufacturers' vehicles' on-board diagnostic systems would require a number of steps: (a) OEMs, independent repair representatives, aftermarket suppliers, and other auto industry participants would need additional certainty about what section 2 requires (*e.g.*, the scope of standardization, and whether all "vehicle networks" would be included); (b) they would

need to agree upon "standards" that could be used on authorization systems, taking into consideration cybersecurity issues, the differences between OEMs' vehicle architectures, and different aftermarket service providers' needs; (c) they would need to form the relevant "unaffiliated entity" and agree upon how to administer, fund, and govern such an entity; and (d) GM and other OEMs would need to design, build, and test vehicles to ensure that the third-party authorization system would work. I am not aware that the Auto Care Association (ACA) has made any progress on its lucrative plans to establish such a third-party governance entity. Nor am I aware of any steps to create such an entity since the passage of the Data Access Law.

Section 3: Disabling the Telematics System

27. The Attorney General suggests that GM could immediately "comply" with Section 3 of the Data Access Law by disabling the telematics systems in its vehicles. *Id.* ¶ 198. Doing so would reduce consumer choice, as customers would lose their ability to buy GM cars with enabled telematics in Massachusetts, and deprive them of the ability to purchase important services that many GM customers choose for their vehicles. In GM's case, the telematics system is its OnStar service that GM has agreed contractually to provide to current drivers who have chosen to use OnStar. In any event, I do not know whether deactivating OnStar would constitute "compliance" with Section 3 of the Data Access Law or simply avoid compliance with that provision. However, disabling OnStar on GM vehicles in Massachusetts would eliminate several important services that GM customers have chosen for their vehicles.

28. For instance, OnStar includes emergency response and automatic crash response features that permit GM vehicles and their owners to immediately contact emergency services if they have an accident, experience a medical emergency, or otherwise need immediate assistance. Likewise, as noted above, OnStar permits FOTA updates that allow GM vehicle owners to

immediately update the software on their vehicles. OnStar subscribers also enjoy other benefits, such as roadside assistance, stolen vehicle assistance, navigation services, remote key entry, and vehicle location services.

29. In short, disabling OnStar on GM vehicles in Massachusetts would come at the expense of features that enhance the safety, security, and convenience their vehicles provide.

Section 3: Equipping the Vehicle with a "Dongle"

30. The Attorney General suggests that GM could attempt to comply with Section 3 of the Data Access Law by equipping the GM vehicle with a wireless "dongle" that could "send any necessary commands for diagnosis and repair." *Id.* ¶¶ 209-10. This poses major cybersecurity problems. As NHTSA has explained in its most recent cybersecurity guidance, "Wireless interfaces into vehicle systems create new attack vectors that could potentially be remotely exploited." 2022 NHTSA Cybersecurity Best Practices § 8.7. That same guidance notes that dongles and other devices connected to OBD-II ports could create "risks . . . when connected with vehicle systems" and should be given only "appropriate *limited access*." *Id.* § 6.1 (emphasis added). And the Attorney General's own expert admitted at trial that vehicles could be "hacked" using wireless dongles. Even putting aside the major cybersecurity risks posed by a "dongle," however, GM cannot comply using the Attorney General's "dongle" solution for a number of reasons.

31. For instance, I understand that the parties agree that a "platform" refers to "a vehicle's architecture and associated software and features." Assuming that definition is correct, then inserting a dongle into GM vehicles' existing OBD-II ports does not create an "inter-operable, standardized, and open access platform," as Section 3 of the Data Access Law requires. Rather,

GM vehicles' platforms would remain non-standardized and GM-specific, without "open access" to any user.

32. Further, under the Attorney General's solution, the "dongles" would need to be secured with a key that is administered by an entity that is unaffiliated with an OEM. AG PFOF ¶ 218. This poses the same problem described above with respect to Section 2—namely, that creates untenable cybersecurity risk, no such entity currently exists, GM cannot develop such an entity, and there are major barriers that must be overcome before such an entity could be created.

33. Relatedly, to attempt to comply with the "standardized" requirement of Section 3, the Attorney General proposes using the Unified Diagnostic Services (UDS) protocol and Secure Vehicle Interface (SVI). *Id.* ¶¶ 210, 233. However, GM, like most OEMs, has a number of diagnostic, maintenance, and repair functions that do not use UDS. Likewise, SVI is only a theoretical mechanism for establishing a secure transmission—not one that has been developed, tested, or implemented in practice. Even the Attorney General's proposed SVI mechanism would require development of a "data dictionary" that could translate between GM vehicle-specific messages and standardized external messages, but that data dictionary does not exist, and it would need to be developed by tool vendors—not GM or any other single manufacturer. I also recall from the trial that NHTSA informed the ACA that it likely would not be possible to establish the certificate authority necessary for SVI.

34. In addition, there are other significant technical problems that prevent the implementation of the Attorney General's "dongle" solution on GM vehicles. For one, GM's OBD-II ports are not designed for, or intended to, wirelessly transmit large amounts of vehicle data. That is even more true if the "mechanical data" to be transmitted encompasses not only diagnosis, maintenance, and repair data, but also any other vehicle data that could have some

bearing on diagnosis, maintenance, and repair issues. I also am not aware of any manufacturer that makes (or could make) a "dongle" equipped to transmit data from GM vehicles in the manner that the Attorney General suggests. Further, GM does not have a "mobile-based application" that could be used in conjunction with the "dongle." Therefore, GM would need to start from scratch to both make technical changes to its vehicle architecture and develop new devices and software—and it cannot do so before knowing with more certainty what Section 3 actually requires and before some entity manufactures the proposed dongle.

Section 3: Fully Telematic Diagnostic Platform

35. The Attorney General alternatively proposes that GM could design and implement a "telematic platform" built into the vehicle architecture. *Id.* ¶ 222. Again, enabling diagnosis, maintenance, and repair functions through telematics systems creates another attack vector into vehicles. 2022 NHTSA Cybersecurity Best Practices § 8.7. However, even beyond cybersecurity issues, GM cannot attempt to comply with Section 3 using this proposed "solution" because: (a) the proposed telematics platform assumes the development of SVI, which is a theoretical concept that has never been developed, implemented, or tested in practice, and is contingent on other industry representatives creating a so-called "data dictionary"; (b) even once that "data dictionary" is developed, the proposed telematics platform and accompanying "mobile-based application" would require years of design and development, which GM could not undertake without additional certainty about what Section 3 actually requires; and (c) it appears that the Attorney General's proposed solution still would not constitute an "open access" platform, as Section 3 of the Data Access Law mandates.

Conclusion

36. To summarize, throughout the trial and since, I carefully considered the Attorney General's proposed method of compliance. I again determined that GM cannot comply with the Data Access Law and meet its federal law obligations. There also still are significant uncertainties about what the Data Access Law requires, and there are a number of prerequisites (including the third-party and certain "standardization" and creation of independent, industry-wide entities) that must be created before GM can attempt to implement the Data Access Law. In the meantime, GM already provides consumers with an ability to choose which providers service their vehicles, and it does so while ensuring that its vehicles are subject to strong cybersecurity controls.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: October 21, 2022

Kevin Tierney

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on the date of electronic filing.

/s/ Laurence A. Schoen
Laurence A. Schoen