Exhibit B

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

Affidavit of Gregory Potter

I, Gregory Potter, hereby depose and say of my personal knowledge as follows:

I. Background

1. I am Chief Technology Officer of the Equipment and Tool Institute ("ETI").
2. ETI is a trade association of automotive tool and equipment manufacturers and technical information providers that was founded in 1947. ETI's mission is to advance the vehicle service industry by providing technical data and open dialogue between the manufacturers of transportation products, government regulators and the providers of tools, equipment and service information."
3. ETI is an independent organization that is unaffiliated with any original equipment manufacturer, or "OEM".
4. I have been involved with ETI since I joined the Board of Directors in 1997. I served on the Board of Directors from 1997–2014 (including a term as President of the Board of Directors from 2004-05), and as Executive Manager from 2014–19.

5. I have over 35 years of experience in the automotive industry. I have been a full member of SAE International (formerly the Society of Automotive Engineers), a professional organization and standards body, since 1995. I have participated in over 25 Committees affiliated with SAE and the International Organization for Standardization ("ISO"), an international standard-setting body that promotes commercial standards. From 2006–2013, I served on the Board of Directors for the Inter-Industry Conference on Auto Collision Repair ("I-CAR International"), an international not-for-profit organization dedicated to providing the information, knowledge, and skills required to perform complete, safe, and quality repairs.

6. I have also been involved with the National Automotive Service Task Force ("NASTF") since its inception. I am currently the Treasurer and a member of the Executive Committee of NASTF. NASTF was established in 2000 to identify and resolve gaps in the availability and accessibility of automotive service information and training. Its primary focus is to facilitate connections between independent auto repair professionals and automakers. I have also worked as Director of Sales, Automotive, and Heavy Duty at DG Technologies from 2008–14, Director of Global Product Management & Development at Chief Automotive Technologies from 2003–08, Director of OEM at Snap-on Tools from 1996–2003, and Account Manager at SPX Corporation from 1992–96.

7. I hold a Master's Degree in Business Administration and a Bachelor's of Science in Electrical Engineering from Lawrence Technological University, as well as an Associate of Science Degree in Mechanical Engineering from Schoolcraft College.

II. Overview

8. Based on my position and experience, I have personal knowledge of the history and current state of data and functionality provided by vehicle manufacturers for use in diagnostics, repair, and maintenance, including technical and logistical provision of such data and functionality to aftermarket scan tool companies and independent repair shops.

9. My testimony addresses the current setup of the diagnostic scan tool industry and relationship between vehicle manufacturers and independent repair tool manufacturers. This information provides the basis for understanding the technical and logistical changes required by the 2020 Right to Repair Law. This factual information about diagnostic scan tools, existing vehicle security features, and the role that ETI plays in providing information between vehicle manufacturers and the aftermarket provides important context for understanding how complying with the 2020 Right to Repair Law would affect the automotive industry.

10. To evaluate the impact of the 2020 Right to Repair Law on emissions standards and safety-critical vehicle functions such as braking and steering, it is essential to understand the different type of information currently available to independent repair facilities, how that information is made accessible, how diagnostics and repairs are performed using scan tools, and how ETI serves as an intermediary that provides information received from a majority of vehicle manufacturers to ETI members comprised largely of aftermarket scan tool companies and dongle manufacturers.

III. Regulated Data and the J-1962 Connector

11. Section 2 of the 2020 Right to Repair Law concerns “access to vehicle on-board diagnostic systems . . . .” Based on my industry experience, requiring access to the “on-

board diagnostic systems" means access to all on-board diagnostic data, including both regulated data and enhanced diagnostic data, discussed in further detail below.

12. Since 1996, vehicles have been required by Clean Air Act regulations and requirements developed by the Environmental Protection Agency and California Air Resources Board to make certain emissions-related data available for state emissions testing. This "regulated" data provides information on whether a vehicle is operating in accordance with emissions requirements, but does not provide all information necessary for diagnostics, maintenance, and repair.

13. Regulated data is required to be made available through the OBD-II specification. The OBD-II specification is the second generation of OBD, which stands for "on-board diagnostics." The OBD-II specification is the standard methodology for accessing emissions-related vehicle diagnostic information.

14. The OBD-II specification provides for a standardized hardware interface, the SAE J-1962 connector. The J-1962 connector is a female 16-pin port, on which particular pins need to be able to provide the required emissions-related data. Other pins on the connector are not regulated, and each OEM is free to choose the information to be made available, the electronic signaling protocols, and the messaging format for each of these manufacturer discretionary pins.

IV. Enhanced Diagnostic Data

15. In addition to regulated data, vehicles contain "enhanced" diagnostic data, which provides information and functionality necessary for vehicle diagnostics, maintenance, and repairs. Most OEMs, including FCA and GM, have chosen to provide some of the

enhanced diagnostic data using the free pins (manufacturer discretionary) of the J-1962 connector.

16. Enhanced diagnostic data can be separated into two general forms.

17. First, enhanced diagnostic data includes a set of pre-defined diagnostic trouble codes (DTCs), which, upon request by a scan tool, describe a diagnostic problem with a vehicle. Regulated DTCs are standardized pursuant to SAE J-2012, which provides a DTC format and a description of the standardized set of DTCs. In addition to regulated DTCs, each manufacturer can design their own proprietary DTCs. Acquiring a DTC from a vehicle is often referred-to as a "read" operation, because it consists simply of sending a request to read information provided by the vehicle.

18. Second, enhanced diagnostic data includes read operations and a set of pre-defined "commands" that, more precisely, request the vehicle to perform a certain action related to diagnostics, repair, and maintenance. Sending such a command to a vehicle is often referred-to as a "write" operation, because it consists of affirmatively changing, in some small way, the status of the vehicle. An example of a write operation is requesting that the malfunction indicator lamp (also known as the check engine light) shut off after a repair is made. Another common type of command sent by scan tools are "functional routines," which request that a vehicle component take an action so a repair person can identify which part of a component is triggering the DTC or to verify that a newly replaced part is working properly.

19. The ability to send both "read" and "write" options is often referred to as "bidirectional" operations.

20. Pursuant to the 2013 Massachusetts Right to Repair Law and the 2014 memorandum of understanding (MOU) among participants in the automobile industry, most (not all) enhanced diagnostic data must be made accessible to vehicle owners and non-OEM-affiliated repair shops. Such access is achieved using a scan tool.

V. Types of Scan Tools

21. Scan tools are currently able to both receive information and send commands to in-vehicle components for purposes of maintenance, diagnostics, and repair (though, as described at paragraphs 53–60 below, some OEMs have begun limiting the scope of commands that scan tools can send without additional manufacturer authorization).

22. Currently, different types of diagnostic scan tools are able to access different data on a vehicle.

23. Engineering tools, which are used by the OEMs to develop their vehicles, can manipulate everything necessary to develop and test a vehicle, including reading and writing requests, reprogramming, and reconfiguring electronic control units, or “ECUs”. ECUs are modules that control one or more of a vehicle’s electrical systems or subsystems. The number of ECUs in a vehicle varies based on a vehicle’s features and can range from a few dozen to over one hundred.

24. Dealership tools, which are used at car dealership service facilities, can send requests to read and write data and perform some reprogramming and reconfiguring functions. A dealership tool has a smaller scope of capabilities compared to an engineering tool because it is primarily designed for vehicle repair functions, as opposed to engineering and development functions.

25. Aftermarket tools, which are developed by independent scan tool companies—often ETI members—can send read and write requests. The capabilities of each aftermarket tool depend on the individual tool and the permissions provided by each OEM. ETI is often able, through negotiation with each OEM, to obtain the information necessary for a scan tool to perform the same functions as a dealership tool. Some types of requests that have been deemed "intrusive" by an OEM are inaccessible unless the aftermarket users seek manufacturer authorization to bypass the secure gateway, discussed in greater detail in paragraphs 53–60 below.

26. As noted, many of ETI's members today are diagnostic scan tool companies. ETI serves as an intermediary that disseminates data from vehicle manufacturers to these companies that produce aftermarket scan tools.

27. OEMs that work with ETI provide ETI with the technical information for their vehicles about where a vehicle's specific modules are located, what communication protocols each ECU uses, and what parameters and DTC's it supports for both regulated and enhanced diagnostics.

28. Vehicles contain multiple communication networks that may or may not use the same physical layer, baud rate or protocol. Typically, these separate networks communicate with each other via gateway modules that connect the networks together and/or translate the data if it is in different formats. The technical information that OEMs provide ETI includes, among other things: which modules are located on which bus, a list of parameters for each module, instructions to interpret module responses and convert module responses into different formats, which communication protocol is used by each ECU, the address for each ECU, and any necessary security information.

29. Once ETI receives the technical information from the OEMs, ETI provides its members with the information, and its members use the information to create diagnostic scan tools for the aftermarket. The information provided by the OEMs allows scan tool companies to create tools that can decode proprietary OEM diagnostic messages.

30. ETI runs a background check on new members to ensure that they are a legitimate company. ETI members pay an annual membership fee. The OEMs are not involved in the process of admitting a new ETI member.

31. The ETI background check requires ETI members to be "engaged as a manufacturer or marketer of automotive service tools and information, financially sound, have a reputation for integrity and sound character, and to meet other such requirements as established by the board of directors."

32. Some OEMs require the scan tool companies to sign end user license agreements governing how the company will use the information provided by ETI. For example, Fiat Chrysler Automobiles (FCA) (now technically Stellantis) requires ETI members to sign a licensing agreement.

33. Some OEMs do not require end user license agreements, and simply allow ETI to decide which companies to provide the information to. For example, Mitsubishi currently falls within this category of companies that do not require ETI members to sign a licensing agreement to receive the technical information for their scan tools.

34. A few OEMs do not use ETI as an intermediary. General Motors (GM) is one company that does not use ETI, and instead enters into its own licensing agreements with scan tool companies.

VI. UDS Messages and Functionality

35. Although OEMs have agreed pursuant to the 2014 MOU to make enhanced diagnostic data accessible to vehicle owners and non-OEM-affiliated repair shops, the specific manner in which that data must be made available is not specified. Enhanced diagnostic data is made available through the regulated and/or unregulated pins on the J-1962 connector. Those unregulated, manufacturer discretionary pins, as I note above, are designed differently by each OEM.

36. Most vehicle manufacturers, however, make enhanced diagnostic data available using Unified Diagnostic Services ("UDS"), a communication protocol specified in the ISO 14229 set of standards and used in automotive ECUs. A communication protocol is a system of rules that creates a format for exchanging messages. UDS defines how the diagnostic message is created, handled, and delivered, but does not define the contents of the message, which is proprietary to each OEM. UDS has become the *de facto* standard for enhanced diagnostic data in part because OEMs invariably obtain their ECUs from the same Tier 1 suppliers.

37. UDS messages may be sent to appropriate ECUs within a vehicle by a scan tool connected to the vehicle through its J-1962 port. Vehicles typically recognize when a scan tool or other device is connected to the J-1962 port, because the vehicle detects that a new module has been connected to its network.

38. UDS messages use a request-response format. This means that the scan tool sends a request to read or write diagnostic data, the vehicle receives the request, and the vehicle sends back a response. The vehicle may respond by providing the requested DTC(s) or performing the requested action(s). Alternatively, the vehicle may respond by refusing to

perform the requested function. Some common reasons for a vehicle to reject a request include: specific conditions required for performing the function are not met, the request format is invalid, security access is denied, or the requestor has exceeded the number of permissible attempts to make a request.

39. Specifically, vehicles are designed with “rationality” controls that specify necessary conditions for a request to be carried out. A common response code is “conditions not met,” which signifies that rationality controls programmed into the vehicle are not met. For example, a command to disable the brakes while the vehicle is driving would trigger a response that the conditions are not met for the request because the vehicle is not stationary, which would be part of the criteria for a safe state for that function to be carried out as defined by the OEM. Rationality controls are selected and programmed by each OEM, and are not necessarily consistent across multiple OEMs, or even across multiple vehicle models manufactured by the same OEM.

40. UDS messages (service messages) are different from the vehicle’s operational Controller Area Network (“CAN bus”) messages, which are proprietary to the OEMs. A vehicle CAN bus is a high-speed vehicle network that can be used for communications between ECUs. Diagnostic scan tools now typically connect through the J-1962 connector to a diagnostic gateway module that connects to the different networks on the vehicle. The gateway will pass the diagnostic requests to the appropriate network for processing. This way the in-vehicle network (IVN) can provide a method for diagnostics without having every network connected to the J-1962 connector and separate the actual network from being accessed directly from the J-1962 connector. This method provides the OEM’s

IVN security by prohibiting direct access to a specific network where a non-authorized message could be put on the network.

41. Scan tools' ability to send commands to a vehicle does not include the ability to reprogram a module. A module can only be reprogrammed by obtaining the OEM's software application and a J-2534 tool. The J-2534 tool is an interface device that connects to a laptop to provide information from the OEM to the vehicle. Reprogramming is a different function beyond the scope of enhanced diagnostic data necessary for maintenance, diagnostics, and repair.

42. Scan tools' ability to send commands to a vehicle does not include the ability to reconfigure a module. Similar to reprogramming, reconfiguring a module can only be done with the OEM's software and a J-2534 tool. Reconfiguring is a different function beyond the scope of enhanced diagnostic data necessary for maintenance, diagnostics, and repair.

VII. Security of J-1962 Port– Service 27

43. Up until a few years ago, the J-1962 port had no security in place to prevent a scan tool or any other device from directly sending non-authorized messages onto the network.

44. Security over enhanced diagnostic functions historically has been achieved through use of Service/Mode 27 (Service and Mode terms get used interchangeably in diagnostics). Service 27 is a secure access mode of scan tool operation that runs through a designated pin on the J-1962 port and prohibits access to certain enhanced diagnostic functions (read and/or write) without a key.

45. Service 27 is a security function of the module that is receiving a request.

46. OEMs decide what diagnostic functions are locked behind Service 27 requests and how complex a Service 27 key to use.

47. OEMs that work with ETI provide the key necessary to unlock Service 27 to ETI, which in turn provides it to its members. ETI's members code the key 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.

48. Most Service 27 codes today use seed and key security. This seed and key security information can be embedded directly into a scan tool so that there's no need to contact the manufacturer each time a repair is made.

VIII. Security – Diagnostic Gateways and Secure Gateway Modules

49. OEMs that work with ETI provide ETI with the necessary security-related information needed for scan tools to perform diagnostics and repairs. Because of the role ETI plays as an intermediary between the OEMs and scan tool companies, I have personal knowledge of some existing vehicle security access requirements, including diagnostic gateways and secure gateway modules.

50. Within the past few years, most vehicles have implemented a type of diagnostic gateway so that the pins on the J-1962 port do not have active network lines connected to them. Instead, the diagnostic scan tool sends a request to the diagnostic gateway, and the gateway sends back a response that, if appropriate, includes the enhanced diagnostic data. This method has been used in addition to Service 27.

51. A diagnostic gateway in this context is a function of a single module, whereas Service 27 is a security function emanating from existing, typically multiple, vehicle modules.

52. Toyota, Ford, and FCA did not have any diagnostic gateway in their vehicles until just a few years ago. This meant that a diagnostic scan tool or any capable device could access any information on any network on the vehicle if the proper commands were sent or put any message on the network that it chose to send.

53. Beyond diagnostic gateways, within the past several years, some OEMs have begun implementing "secure gateway modules" (SGWs) as a manufacturer authorization system for accessing some or all enhanced diagnostic functions. Secure gateways prohibit access to certain diagnostic functions unless a repair shop is registered and authenticated through a secure device. Access to secure gateways is typically managed by a certificate process, which requires a scan tool to be connected to the vehicle and to the internet, creating a point-to-point connection between the vehicle and the manufacturer's server, for authorization.

54. Vehicles using a secure gateway typically allow owners and independent mechanics to read most of the data from the vehicle, but do not allow commands to be sent to the vehicle.

55. Each OEM determines what diagnostic requests are considered "intrusive" and blocked by the secure gateway, such that it is inaccessible without manufacturer authorization each time the function is sought. There is no uniformity among OEMs as to what functions are locked out by each OEM's secure gateway.

56. FCA currently incorporates a secure gateway in all or nearly all of its makes and models. Some models of Mercedes-Benz, Hyundai, Kia, and Nissan also incorporate a secure gateway. It is my belief, based on my knowledge of the industry and my discussions with

OEMs, that other OEMs are planning to start incorporating secure gateways into their vehicles.

57. There is currently no standardization of the secure gateways.

58. FCA's secure gateway requires scan tool device and user registration through their "AutoAuth" system, which is a public key infrastructure administered by Integrity Security Services, LLC. Once registered and authorized by the "AutoAuth" system, approved enabled diagnostics platforms using current software are allowed to perform functions otherwise locked behind the secure gateway.

59. To access the diagnostic functions protected by FCA's secure gateway, the diagnostic scan tool, independent repair shop, and individual mechanic making the repair must be registered with the FCA system. This secure gateway access only unlocks the module for a current diagnostic session. This means that secure gateway access is only good for a certain period of time for that particular vehicle's repair, and access will end if the current diagnostic session is ended. The authorization process must be repeated for each diagnostic session and individual repair on each different vehicle, as well as if the current diagnostic session is disrupted by something like the tool being disconnected or a period of inactivity.

60. FCA's secure gateway prevents independent repair shops from using Service ID 14, "erase all codes." This prohibits independent repairers from erasing enhanced diagnostic trouble codes without manufacturer authority, which is necessary to reset trouble code lights such as the service light after a repair is made.

IX. Dongles

61. Several ETI members are manufacturers of dongles, which are devices that can connect to the J-1962 port to provide vehicle information to another entity for different purposes. Common dongle purposes include the provision of driving performance information for insurance companies and vehicle fleet management.
62. Some existing ETI members create dongles that provide some enhanced diagnostic information. These include, for example, GeoTab, Bluedriver, and Voyomotive.
63. Dongles, which operate similarly to scan tools, have the capacity to send commands to a vehicle.

Signed under the pains and penalties of perjury.

Date: 5/26/21

_/s/ Greg Potter__

Gregory Potter