KENNETH A. KUWAYTI (CA SBN 145384)
KKuwayti@mofo.com
BERKELEY G. FIFE (CA SBN 325293)
BFife@mofo.com
MORRISON & FOERSTER LLP
755 Page Mill Road
Palo Alto, California 94304-1018
Telephone: 650.813.5600

JOHN R. LANHAM (CA SBN 289382)
JLanham@mofo.com
JANET S. KIM (CA SBN 313815)
JKim@mofo.com
MORRISON & FOERSTER LLP
12531 High Bluff Drive
San Diego, California 92130-2040
Telephone: 858.720.5100

Attorneys for Plaintiffs
MITCHELL REPAIR INFORMATION COMPANY, LLC and SNAP-ON INCORPORATED

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

MITCHELL REPAIR INFORMATION COMPANY, LLC, a Delaware limited liability company, and SNAP-ON INCORPORATED, a Delaware corporation,

Plaintiffs,

v.

AUTEL. US INC., a New York corporation, and AUTEL INTELLIGENT TECHNOLOGY CORP., LTD., a Chinese corporation,

Defendants.

Case No. **'21CV1339 CAB BGS**

COMPLAINT

JURY TRIAL DEMANDED

Mitchell Repair Information Company, LLC ("Mitchell 1") and Snap-on Incorporated ("Snap-on") (collectively, "Plaintiffs") bring this action against Defendants Autel. US Inc. ("Autel US") and Autel Intelligent Technology Corp., Ltd. ("Autel ITC") (collectively, "Defendants" or "Autel") and allege as follows:

NATURE AND SUBSTANCE OF THE ACTION

1. This case arises out of the blatant theft of Plaintiffs' proprietary information and data by Defendant Autel US and its Chinese parent company, Defendant Autel ITC.

2. Plaintiffs Snap-on and Mitchell 1 provide proprietary diagnostic and repair information that automotive technicians use to facilitate the efficient repair of automobiles and trucks. This information is based on expert and artificial intelligence analysis of literally billions of data points that Plaintiffs have gathered from real world repair information accumulated over a period of more than 25 years. Plaintiffs have spent over $100 million dollars on research, analysis, and product development relating to this proprietary information over many years. No other company in the world has access to even a small fraction of this volume of real world repair data, and, as a result, no other company offers a product that provides as comprehensive and detailed diagnostic and repair information.

3. Snap-on and Mitchell 1 offer a variety of products that allow end users to access some of this information when conducting their repairs, in exchange for a monthly subscription fee. As discussed in more detail below, these products range from a custom handheld diagnostic computer that connects directly to the vehicle and sells for an MSRP of just under $10,000, to separate web-based services for vehicles and for medium and heavy trucks that allow users to access some of this proprietary information online. Plaintiffs' products combine access to their proprietary information with comprehensive Original Equipment Manufacturer ("OEM") information, much of which requires Mitchell 1 to pay substantial annual licensing fees.

4. Autel competes with Snap-on and Mitchell 1, and has its own handheld diagnostic computer tool. But it does not have access to anywhere near the same level of real world repair information. Further, Autel has not invested the years of time and money that would be required to analyze and usefully categorize this repair information. Instead, Autel decided to steal the information from Snap-on and Mitchell 1.

5. Autel US and Autel ITC have done so by improperly syphoning data from three separate products, in at least three different ways: (1) circumventing the security measures on Plaintiffs' handheld diagnostic computers to "spoof" those devices and engage in mass, automated downloads of Plaintiffs' proprietary information; (2) stealing the user name and password of a different company to surreptitiously and systematically pull Plaintiffs' proprietary data from its online TruckSeries product, which provides diagnostic and repair information for medium and heavy trucks; and (3) improperly pulling large quantities of Plaintiffs' proprietary information through Mitchell 1's ProDemand product in violation of the terms of that product's End User License Agreement.

6. This theft of vehicle repair data is part of a familiar pattern for Autel. It has been sued twice before by Ford and by GM for stealing their repair-related information.

7. Autel has concealed its conduct by, among other things, masking its attacks on Plaintiffs' data by using more than 300 different IP addresses, copying the authentication information from Snap-on's handheld diagnostic devices, pretending to be making requests for data through over four hundred devices, and secretly operating behind the username and password of a different registered user. Plaintiffs have taken countermeasures to stop this conduct, but Autel has morphed its behavior in return and, undeterred, continues to try to steal Plaintiffs' data.

8. Snap-on and Mitchell 1 accordingly bring this action for temporary, preliminary, and permanent injunctive relief to stop Autel from making use of the

information it has taken and from taking any further data, and for damages for Autel's flagrant violations of law.

PARTIES

9. Plaintiff Mitchell 1 is a Delaware limited liability company with its principal place of business at 16067 Babcock Street, San Diego, California 92127.

10. Plaintiff Snap-on is a Delaware corporation with its principal place of business at 2801 80th Street, Kenosha, Wisconsin 53143.

11. Defendant Autel US is a New York corporation with its principal place of business located at 175 Central Ave., Suite 200, Farmingdale, New York 11735. Upon information and belief, Autel US is a wholly-owned subsidiary of Autel ITC.

12. Defendant Autel ITC is a Chinese corporation having a principal place of business at 7th, 8th, and 10th Floor, Building B1, Zhiyuan Xueyuan Road, Xili, Nanshan, Shenzhen 518055, China and having an office in the United States at 175 Central Ave., Farmingdale, New York 11735.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over the claims arising under the Digital Millennium Copyright Act ("DMCA") (17 U.S.C. §§ 1201, 1203) pursuant to 28 U.S.C. §§ 1331 and 1338.

14. This Court has subject matter jurisdiction over the claims arising under the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030) pursuant to 18 U.S.C. § 1030(g) and 28 U.S.C. § 1331.

15. This Court has subject matter jurisdiction over the claims arising under the Defend Trade Secrets Act ("DTSA") (18 U.S.C § 1836) pursuant to 18 U.S.C. §§ 1836(b) and 1837, and 28 U.S.C. § 1331.

16. This Court has supplemental subject matter jurisdiction over the related state law claims pursuant to 28 U.S.C. § 1367 because these claims are so related to the federal claims that they form part of the same case or controversy

under Article III of the United States Constitution and derive from a common nucleus of operative facts.

17. This Court has an independent basis for jurisdiction over all the claims herein in accordance with 28 U.S.C. § 1332 because there is diversity of citizenship between the parties, and the amount in controversy exceeds $75,000.

18. Defendants are subject to personal jurisdiction in this District because this action arises out of Autel's illegal conduct that intentionally targets and causes injury to Plaintiffs in this District. For example, as further detailed in the allegations in this Complaint, Autel has circumvented Plaintiffs' security measures to illegally obtain access to, and make unlawful use of, Plaintiffs' proprietary diagnostic and repair information hosted by, and stored in, servers located in this District. Autel has also illegally obtained access to, and made unlawful use of, Plaintiffs' products and services developed and sold in this District. Via these and other actions, Autel has made unauthorized use of Plaintiffs' intellectual property, personal property, and proprietary data that was created in and is located in this District.

19. In addition, Autel US has violated the End User License Agreement that it entered into with Plaintiff Mitchell 1 ("Mitchell 1 EULA") with respect to opening and maintaining an account relating to the ProDemand product. Autel entered into a Mitchell 1 EULA by at least 2016, and reaffirmed its acceptance of Mitchell 1's EULA at least as recently as December 2020. A copy of Autel's 2016 Mitchell 1 order form with the EULA signature page, and a copy of the 2016 Mitchell 1 EULA are attached as Exhibits 1-2. The Mitchell 1 EULA requires that parties to the agreement "agree that jurisdiction of any claim or suit hereunder shall be exclusively the courts located within the County of San Diego, California" and specifically states that, for such claims, both parties to the agreement "hereby submit to the personal jurisdiction of such courts." Exhibit 2 at 76 (¶ 17). Autel US has signed this agreement. *See* Exhibit 1 at 70-71.

20. A copy of Autel's 2020 Mitchell 1 order form with the signature page, and a copy of the 2020 Mitchell 1 "Order Terms and Conditions" are attached as Exhibits 3-4. The Mitchell 1 Order Terms and Conditions state that "[t]he agreement between you ("Customer") and Mitchell Repair Information Company LLC ("Mitchell 1") includes: (i) these Mitchell 1 Order Terms and Conditions; (ii) the Order Form; and (iii) the End User License Agreement as may be updated from time to time ("EULA")[.]" Exhibit 4 at 82 (¶ 1). Autel US has signed this agreement as well, reaffirming its agreement to the Mitchell 1 EULA. *See* Exhibit 3 at 78-79.

21. Accordingly, this Court has exclusive jurisdiction over Mitchell 1's claim against Autel US for breaching the Mitchell 1 EULA by improperly using the ProDemand account for the purposes of determining Plaintiff Mitchell 1's entitlement to preliminary injunctive relief for that claim.

22. In addition, Autel markets, sells, furnishes, and supports its competing diagnostic products and services throughout the United States (a fact which has already been established against Autel in multiple written opinions, *see Service Solutions U.S., LLC, v. Autel. US, Inc., et al*., 2013 U.S. Dist. LEXIS 150036, *11-16 (E.D. Mich. Oct. 18, 2013), *Ford Motor Co. v. Autel. US Inc. et al.*, 2015 U.S. Dist. LEXIS 133201, *32-35 (E.D. Mich. Sept. 30, 2015), *General Motors L.L.C. et al. v. Autel. US Inc. et al*., 2016 U.S. Dist. LEXIS 40902, *10-12 (E.D. Mich. Mar. 29, 2016)) including in the State of California to California residents. Upon information and belief, Autel ITC's competing products are sold and distributed by Autel US in the United States. Autel ITC is aware of where these products are to be sold and distributed by Autel US, and therefore intends that these products be sold and delivered to those locations. Such products are purposefully sold and promoted for sale to customers in California, including customers residing in the Southern District of California.

23. At the public website https://www.auteltech.com, which has a notice identifying Autel ITC as the owner of the site, users in California can access and download software, user manuals, and other materials for Autel's diagnostic tools. Users in California can also purchase Autel's diagnostic tools at this site.

24. Venue is proper in this judicial district under 28 U.S.C. § 1391, at least because a substantial part of the events or omissions giving rise to the claims of this complaint occurred in this district, and a substantial part of property that is the subject of the action is situated in this district.

FACTUAL BACKGROUND

A. Snap-on and Mitchell 1

25. Snap-on has been a leading designer and manufacturer of tools essential to automotive and truck repair since its founding over 100 years ago.

26. Snap-on's industry-leading automotive and truck repair equipment includes both traditional hand tools and cutting-edge portable diagnostic computers. In tandem with the automotive industry's advent of vehicular on-board diagnostic ports in the 1980s, Snap-on developed handheld diagnostic computers capable of interfacing with these ports. These sophisticated devices are able to understand "trouble codes" output by vehicles' diagnostic ("OBD-II") ports, initiate testing within the vehicle relating to these codes, and offer diagnostic and repair solutions to problems causing these codes.

27. For more than 30 years, Snap-on has designed and developed varieties of these handheld diagnostic computers. As discussed more below, these tools' features and capabilities have become increasing sophisticated over the years. For example, Snap-on's diagnostic tools now can display for users a wealth of cloud-hosted proprietary expert diagnostic and repair information and OEM sourced repair information. These and other advances are made possible, in part, by Snap-on's roughly 12,000 employees worldwide, almost a third of whom are part of Snap-on's Repair Systems and Information Group.

28. These advances were also made possible, in part, by Snap-on's acquisition of Mitchell 1 in 1996. Mitchell 1 has been a fixture in the San Diego community for over 100 years, and has established itself as an industry-leading provider of resources to automotive and truck technicians and repair shops.

29. Like Snap-on, Mitchell 1 has long recognized the importance of technological resources for vehicle technicians. In the 1980s, Mitchell 1 began releasing electronic repair information and estimator systems. In 1995, Mitchell 1 released its Manager™ shop management and service writing software to automotive repair shops across the country. This software functions to facilitate customer vehicle repairs and contains features such as cost-estimating tools, integration with electronic parts catalogs, and customer and marketing management functions. This software has gathered repair data for vehicles logged in the system since the mid-1990s.

30. Snap-on recognized the importance of Mitchell 1's offerings and the potential impact Mitchell 1's software and repair data could have on the capabilities of Snap-on's diagnostic devices. As such, since acquiring Mitchell 1 over 25 years ago, Snap-on has closely integrated Mitchell 1's software and repair data into the Snap-on ecosystem. For example, Mitchell 1's Manager software is now sold as a component of the Snap-on product ShopKey®. Mitchell 1's software is used in over 32,000 repair shops nationwide and has become by far the most popular shop management software. As a result of this software's widespread use, Snap-on and Mitchell 1 have gathered billions of vehicle repair records. These records contain information such as descriptions of symptoms, diagnosis, and replacement/repair techniques for all logged vehicle repairs. None of Snap-on or Mitchell 1's competitors appear to have even a fraction of this repair data.

31. Snap-on and Mitchell 1 have used this repair data to develop proprietary diagnostic and repair information. This proprietary information is the result of over 100 million dollars of research, analysis, and product development

based on both expert and artificial intelligence analysis of billions of repair records. As discussed more below, this proprietary information is offered through Snap-on's diagnostic device services, and some of the information is also offered as part of Mitchell 1's standalone paid subscription service, ProDemand.

B. Autel

32. Autel US is the U.S. subsidiary of a Chinese company, Autel ITC. Autel is one of Plaintiffs' main competitors in the automotive diagnostic and repair space. It offers products directed to automotive repair shops, including its own handheld devices. Autel products are available nationwide through AutoZone stores and other distributors. On information and belief, Autel has a U.S. headquarters in New York, where Autel US is located.

33. Autel has been sued twice before for stealing data and intellectual property relating to automotive vehicle repairs. *See General Motors LLC v. Autel. US Inc. et al.*, 4:14-cv-14864 (E.D. Mich.), ECF No. 1 (Complaint) (Dec. 22, 2014), *Ford Motor Co. v. Autel US Inc. et al.*, 4:14-cv-13760 (E.D. Mich.), ECF No. 28 (Second Amended Complaint) (Nov. 11, 2015).

34. In *Ford*, Autel was accused of unauthorized access to and use of Ford's Integrated Diagnostic System ("IDS system"), which includes hardware and software components Ford developed to diagnose problems with Ford vehicles. *See generally*, *Ford*, 4:14-cv-13760, ECF No. 28 (Second Am. Compl.) at 8-37. Ford alleged Autel created a program that circumvented Ford's security measures and provided Autel access to Ford's data. *Id.* at 36-37. Ford alleged Autel then stole this data, which included copyrighted and trade secret material (*id.* at 8-9), and used it in its own products (*id.* at 9-33). Autel's motion to dismiss challenging Ford's claims for copyright infringement, counterfeiting, breach of contract, and trademark dilution was denied. *See Ford Motor Co. v. Autel US Inc. et al.*, 2016 U.S. Dist. LEXIS 85875, *6-8, 10-16 (E.D. Mich. July 1, 2016). But, the parties settled

before final adjudication of Ford's claims. *See Ford*, 4:14-cv-13760, ECF No. 109 (Dismissal Order).

35. In *General Motors*, Autel was accused of unauthorized access to and use of GM's proprietary vehicle servicing software and unauthorized use of GM's trademarks, copyrights, and trade secrets. *See generally*, *General Motors*, 4:14-cv-14864, ECF No. 1 (Complaint) at 12-26. Although the parties settled before GM's claims were decided on the merits, *see id.,* ECF. No. 42 (Dismissal Order), Autel's Rule 12(b)(6) motion to dismiss GM's DMCA, CFAA, trade secret, and unjust enrichment claims was denied. *See General Motors LLC v. Autel. US Inc. et al*., 2016 U.S. Dist. LEXIS 40902, *17-33 (E.D. Mich. Mar. 29, 2016).

C. Snap-on and Mitchell 1 Offer Sophisticated Diagnostic and Repair Products Powered by Proprietary Information and Databases

36. Snap-on and Mitchell 1 offer three different products for diagnostic and repair that are at issue in this lawsuit: diagnostic handheld computers, ProDemand, and TruckSeries.

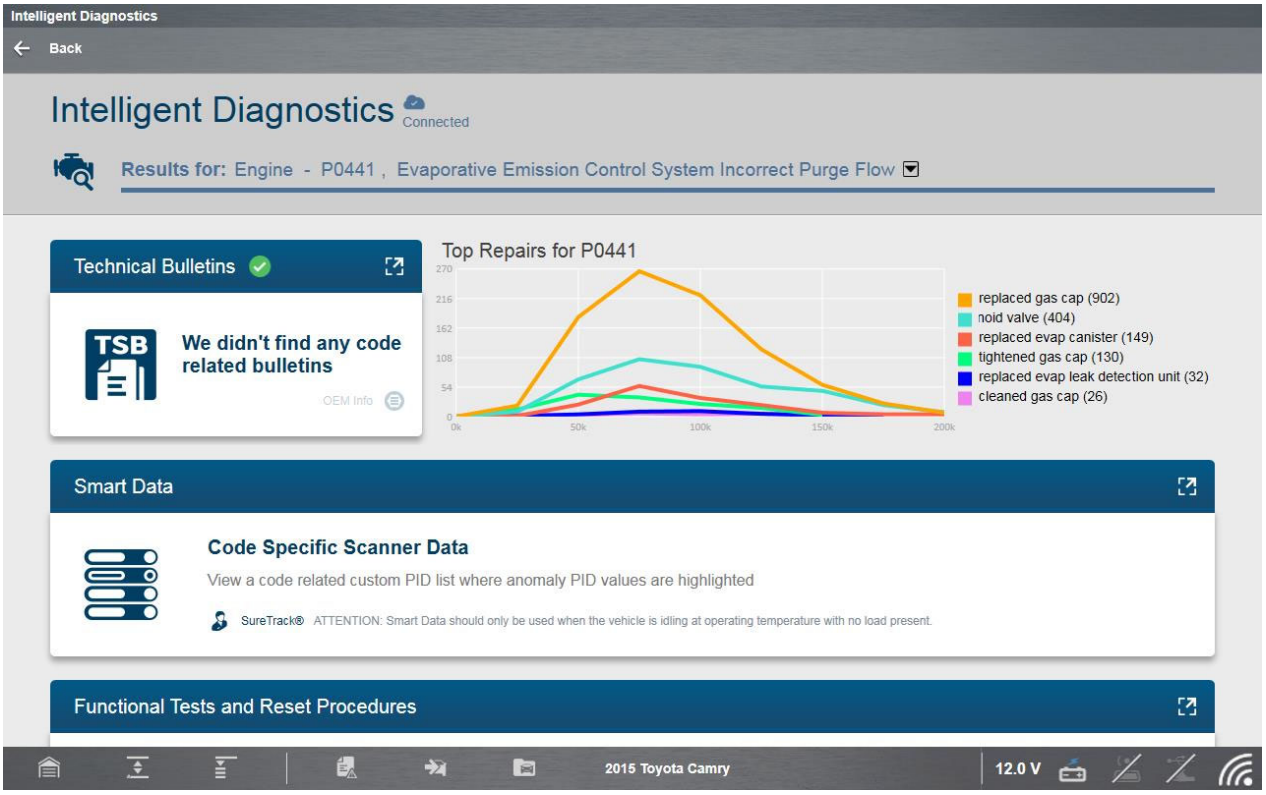
Diagnostic Handheld Computers

37. Snap-on currently offers various types of handheld diagnostic computers. One example is the ZEUS™ device, pictured below, which will serve as an example to illustrate some of the features offered in Snap-on diagnostic systems:

38. This device contains hardware and software allowing it to communicate with a connected vehicle. When connected, ZEUS's scanner function identifies the year, make, model, and engine of the vehicle. The technician may then use ZEUS to scan the vehicle for trouble codes, which are communicated via the vehicle's OBD-II port. After scanning, ZEUS allows the technician to view trouble codes resulting from the scan. The technician can then select to "diagnose" any of those active trouble codes.

39. In response to a technician choosing to "diagnose" an active trouble code, ZEUS provides the technician various types of proprietary diagnostic and repair information relevant to the trouble codes detected on the connected vehicle. As discussed above, this information has been (and continues to be) developed from billions of repair records collected in Mitchell 1's Manager software, and is the result of enormous amounts of Plaintiffs' labor and expenditure. The following represent categories of tailored information that may be displayed to a technician (via "cards" on the ZEUS display) relevant to a vehicle's specific trouble code:

40. Top Repairs: Top Repairs lets a technician quickly understand what the most likely repairs will be for the vehicle at issue. The Top Repair card presents a graph depicting the most common repairs performed for a certain vehicle with certain trouble codes, at particular mileages, along with the frequency of those repairs. An exemplary Top Repairs graph for a P0441 (evaporative emissions) trouble code on a 2015 Toyota Camry appears below:



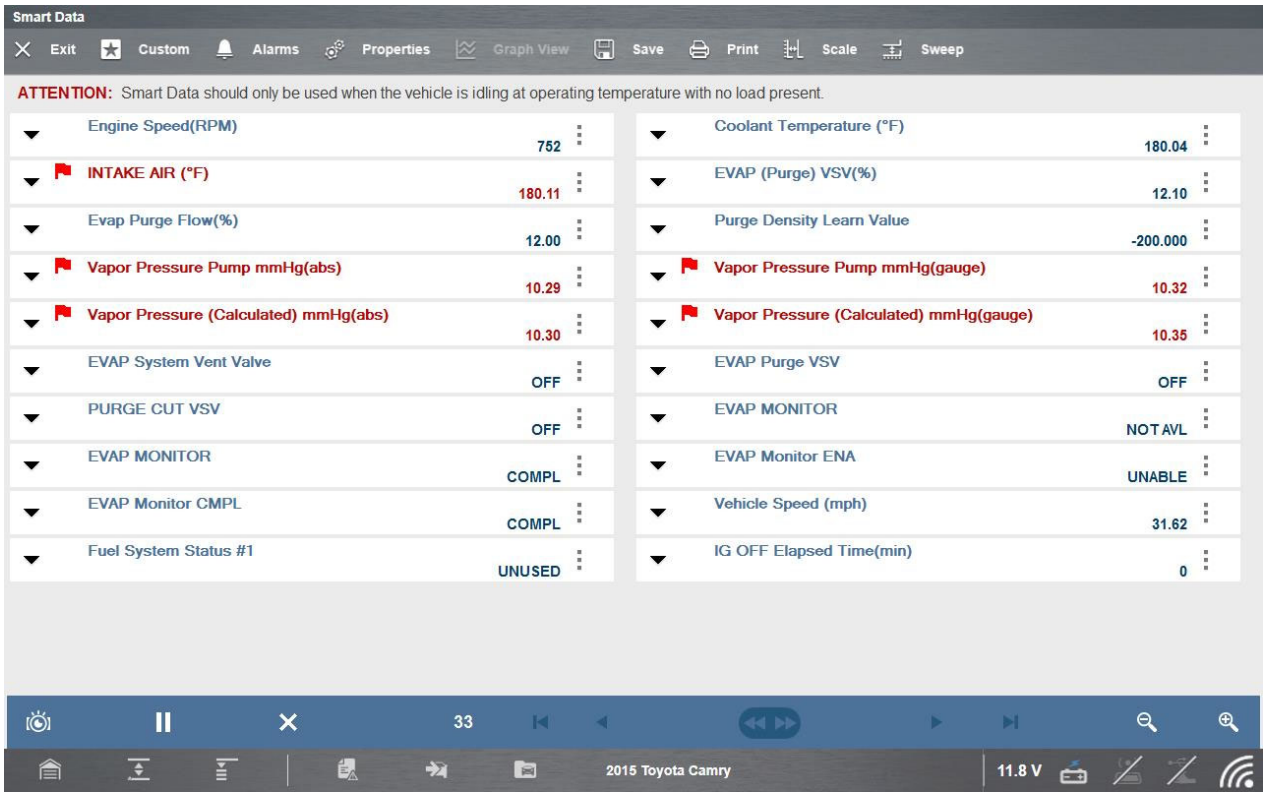
41. This Top Repairs graph is based on a real-world understanding of the most common fixes for a specific vehicle's trouble codes, which is based on Plaintiffs' sophisticated analysis of billions of repair records. Top Repairs therefore can save both the technician and the vehicle owner significant time and money. No other company offers such a comprehensive and specific data set.

42. Real Fixes: Real Fixes provides trouble code-specific recommendations on performing the most common vehicle repairs. These recommendations include information on the behavior associated with the code, the

likely cause (including recommended troubleshooting steps), and the desired results of troubleshooting. Real Fixes includes procedures and tests gathered from real-world repair orders. The narratives for these entries are written by Snap-on expert technicians, who have created millions of unique Real Fix entries. Real Fix data is continually updated and revised to reflect new repair data and new vehicle model years. Each Real Fix card includes a Fixed It count derived from the real-world data. The Fixed It count shows how many times the vehicle problem was solved with the solution described in the Real Fix. Real Fixes are prioritized based on the Fixed It count to help the technician choose the course of action with the highest probability of success.

43. Troubleshooter tips: This card provides tips written by Snap-on expert technicians and other industry experts relevant to the vehicle in question. For example, these tips may include time-saving suggestions for repairs, such as how to determine the most likely components causing a particular problem. Some tips include links to related Functional Tests that further help to diagnose the problem.

44. Smart Data: This card enables technicians to view relevant vehicle Parameter IDs ("PIDs"). PIDs are live readings of a vehicle's systems, which are communicated to ZEUS via a vehicle's OBD-II port from the vehicle's numerous system controllers, which are connected to hundreds of sensors, solenoids, actuators, and switches with associated PIDs. On average, a vehicle may present approximately 100-200 PIDs when connected to a diagnostic scanner, which is too much data to be particularly useful to a technician trying to diagnose a specific issue. But, as a result of years of collecting PID data associated with vehicle repairs and expert analysis of this data, Snap-on has developed lists of PID data points relevant to each trouble code. The Smart Data card presents the technician those PIDS that are relevant to the trouble code at issue.



45. Further, Snap-on has created a "known good" range of values for specific PIDs based on its over 200 billion data points and the views of its experts. The Smart Data card flags specific PIDs that fall outside of Snap-on's "known good range," as shown above. This immediately informs the technician that there is a likely problem with that portion of the system. However, the minimum and maximum values of the "good" ranges for each parameter are not shared with the end user. Snap-on deliberately keeps this information confidential. No competitor has a comprehensive product comparable to Snap-on's PID functionality.

46. Functional tests: ZEUS further displays functional tests associated with a particular trouble code, such as system controls, resets of component operations, and programming new vehicle components. Snap-on's experts, aided by their billions of repair records, have determined which functional tests to associate with particular trouble codes, and have consolidated those relevant tests into a single easy-to-use card.

47. Guided Component tests: This card displays component tests associated with a vehicle's trouble code(s) and guides for how to perform these tests. These component tests are used to determine whether a particular component is good or bad, and are derived from Snap-on's expert analysis of its repair record databases. The narrative step-by-step instructions associated with these test are also prepared by Snap-on expert technicians.

48. Snap-on and Mitchell 1 spend millions of dollars annually to keep the proprietary diagnostic and repair information provided through these cards up-to-date. This proprietary information allows technicians to use Snap-on diagnostic devices to efficiently resolve a vehicle's problem. No competitor has the same volume of repair and diagnostic records, or analysis of these records. Consequently, no competitor is capable of providing technicians a comprehensive catalog of the exact information needed to quickly resolve a particular vehicle's problem.

ProDemand

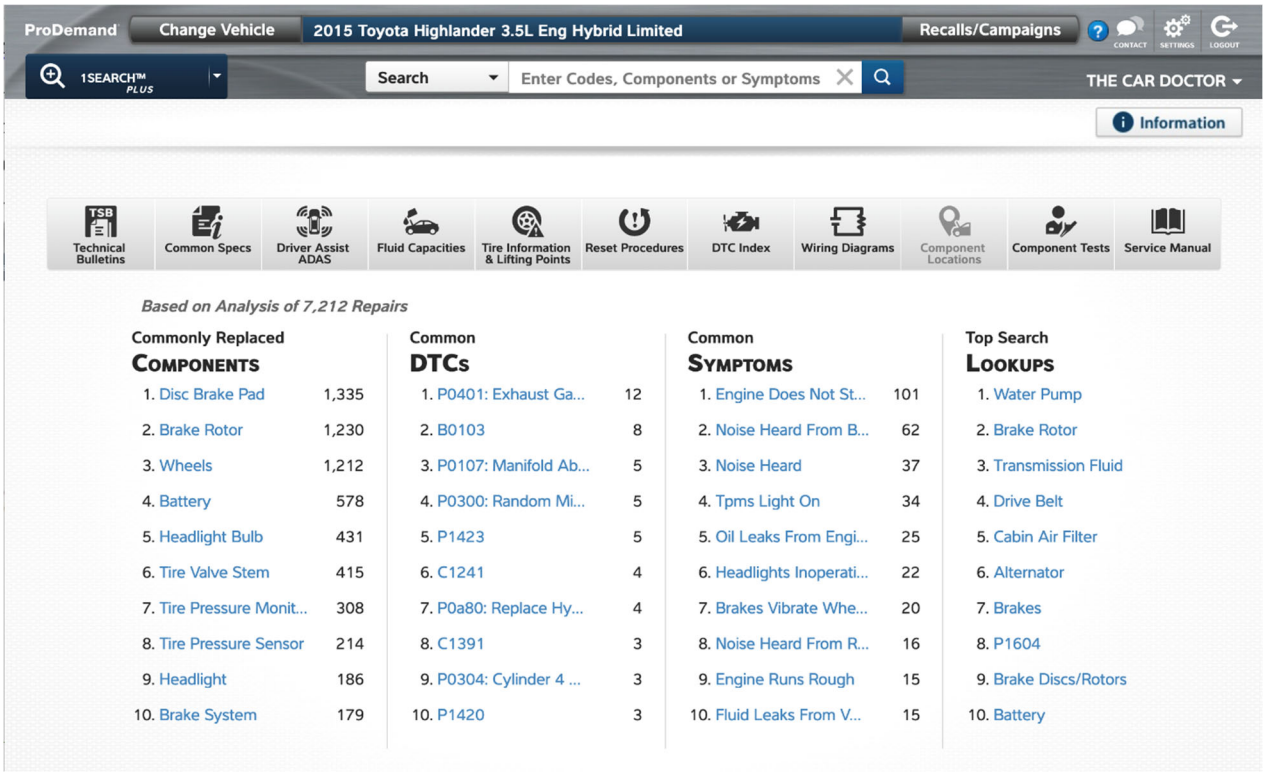
49. Mitchell 1 offers a web-based subscription service that provides diagnostic and repair information for vehicles. ProDemand is available to users only on a subscription basis. Most subscribers must have a valid username and password for access. For some large customer accounts, Mitchell 1 allows the customer to authenticate through a designated specific company IP address, where all of the traffic is routed through their corporate firewalls or routers. Owners of a Snap-on handheld diagnostic device still need to pay an additional subscription fee and open a ProDemand account to make use of the ProDemand features.

50. ProDemand offers its subscribers access to some of the proprietary information described above. In addition, ProDemand organizes and displays comprehensive repair information from vehicle OEMs, including Technical Service Bulletins issued by the OEMs, repair instructions, and calibration information for advanced driver-assistance systems ("ADAS"). Mitchell 1 has to pay significant

fees to license this OEM data. And Mitchell 1 incurs substantial additional labor and expense via its effort to both organize OEM data in a user-friendly manner and to map the OEM information to its own proprietary data services.

51. Mitchell 1's organization and transformation of the OEM data provides significant benefit to users of ProDemand attempting to efficiently access this information. For example, if a user wants to learn about all of the ADAS information for a vehicle, that user would normally have to search for individual items, such as the front view camera, adaptive cruise control, or other sensors on the car. Each manufacturer organizes its information differently, and the information is normally found spread among different component categories, so this is no easy task. With ProDemand, Mitchell 1 avoids this user headache by providing all of a vehicle's ADAS information organized into one place. Mitchell 1 makes this organization consistent for each vehicle manufacturer so that the information is easy to locate. Mitchell 1 also ensures that the same taxonomy can be used across manufacturers, regardless of whether OEMs use different terms for the same component. Mitchell 1 has a team of over 50 people responsible for sorting through all of the OEM data and continually updating and organizing it.

52. In terms of proprietary information, ProDemand allows its users to access Top Repairs, Real Fixes, and Component Tests (described above). ProDemand also offers an additional "Top 10 Repairs" feature (pictured below), which reports the most common symptoms, diagnostic trouble codes ("DTCs"), and most commonly replaced components for a particular year, make, model, engine, and trim for a particular vehicle. This information streamlines a technician's troubleshooting and also allows shops to provide customers with proactive maintenance suggestions to avoid future part failures. The Top 10 Repairs feature is only possible thanks to Plaintiffs' collection of the billions of repair records described above, and the analysis and review of these records by Plaintiffs' industry experts. An example screenshot of the Top 10 Repairs feature is provided below.



TruckSeries

53. Mitchell 1 offers another web-based subscription service, called TruckSeries, which is directed to repair of medium and heavy commercial trucks. It requires a separate paid subscription from ProDemand. To access this service, most subscribers must have a valid username and password. Certain large customers are permitted to authenticate through a specific, designated IP address, as described above.

54. Unlike ProDemand, where most repair information comes from OEMs and is licensed to Mitchell 1, nearly all of the diagnostic and repair information on TruckSeries is authored by Mitchell 1. Mitchell 1 has invested enormous time and effort into TruckSeries.

55. Mitchell 1's efforts, and the resulting proprietary information provided by TruckSeries, saves technicians substantial time and effort when trying to diagnose and repair medium and heavy trucks. Rather than having to go find diagnostic and repair information in lengthy repair manuals from OEMs,

Mitchell 1's system allows technicians to quickly access relevant and applicable diagnostic and repair information and to return specific information to facilitate repairs.

56. For example, a technician who wants to quickly identify the problem that a truck may be experiencing can use the TruckSeries "Top Search Lookups" feature. This feature displays the top ten searches that other technicians have performed for problems they are experiencing on a truck with a particular configuration, giving the technician insight into the most common problems the truck has experienced. The Top Search Lookups is regularly updated as technicians make continued use of TruckSeries.

57. TruckSeries also offers features tailored to a particular trouble code or particular symptoms that a technician has observed with the truck. Some of these features include the following:

58. Testing: This provides a step-by-step narrative on how to diagnose and test a problem.

59. Photos: The Component Connector and Component Location features provide high resolution photographs and CAD drawings that have been created by Mitchell 1 and have been highlighted, color-coded, and labeled where appropriate to display the component and where it fits within the car. These pictures are made by Mitchell 1.

60. Interactive Wiring Diagrams: The original diagrams that contain links to other relevant portions of TruckSeries data to make troubleshooting and repairs easier.

61. Labor Time: This shows estimates of how much time Mitchell 1's experts believe that a repair should take. Unlike automotive manufacturers, heavy truck manufacturers generally do not publish a time for how long they believe a particular repair should take.

62. RepairConnect: This code diagnostic feature allows technicians to enter a vehicle and a trouble code and receive specific repair procedures for the vehicle's problem. The content in TruckSeries is proprietary to Mitchell 1, as Mitchell 1 prepares the diagnostic and repair information itself.

63. TruckSeries also includes ADAS reference tables, torque specifications, step-by-step guidance on how to remove and replace parts, and after repair information describing steps that need to be taken once the repair is completed.

D. Snap-on and Mitchell 1 Spent Years Developing Their Proprietary Data

64. Transforming the billions of repair records collected by Mitchell 1's Manager software into useable, searchable databases has required an enormous undertaking by both Snap-on and Mitchell 1. For this data to be useful, Plaintiffs knew they had to create a set of databases able to associate specific symptoms or trouble codes with specific repairs and component failures, and to associate those pieces of information with the repair, diagnostic, and test information to display to the technician.

65. This task was an immense challenge in part due to the difficulty inherent in organizing and analyzing such a massive volume of data. But the task was made even harder because the underlying repair records were prepared by technicians lacking a common vernacular. For example, technicians across the country often use different naming conventions for vehicle components, use shorthand, or introduce typographical errors or phonetic spellings of vehicle components. There are over *three thousand* variations or misspellings for the term "oxygen sensor" in Plaintiffs' dataset. And some repair records are simply incorrect. To address this, in 2012 Snap-on formed a team of special developers, experts, and editors to solve the problems presented by these service records. The team worked to categorize various terminologies and link related concepts across

the products. Ultimately, the team built a comprehensive taxonomy and ontology to organize repair terminologies across all vehicle makes, models, and engine systems in the databases.

66. Further, reviewing, analyzing, and organizing Plaintiffs' proprietary data so that it can be displayed in a user-friendly form has taken years, and still requires constant human review alongside review by a proprietary artificial intelligence ("AI") algorithm, which employs machine learning and natural language processing to further analyze the processing repair records. This proprietary AI has taken a lead role in data processing and now processes billions of repair records, with constant fine-tuning by human reviewers.

67. As one specific example, Snap-on has expended enormous effort to create and maintain its filtered PID data. Properly-filtered PID data is valuable to technicians because it provides real-time, objective information for various aspects of the vehicle's operation. But a vehicle may display roughly 100 to 200 PID sensors, most of which are not relevant to any given problem. Moreover, technicians typically have no effective way of knowing whether each of the PID values being reported by the car is within the acceptable range. This results in data pollution, making it difficult to use sensor data to diagnose a vehicle.

68. To overcome PID data pollution, Snap-on's experts spent years organizing data for use by repair technicians. This involved creating a proprietary code-to-component metadata structure, with the assistance of proprietary AI technology that associates vehicle problems with probable components, and those components with the relevant PIDs. By utilizing this metadata structure the Smart Data function is able to provide curated PID sensor data for only the most relevant components.

69. Snap-on has also analyzed PIDs and over 200 billion data frames through a combination of human expert analysis and machine learning to determine the normal distributions of PID data, in order to identify minimum and maximum

accepted values, and a "known good" range. This initial process involved millions of dollars in resources. And Snap-on's data continues to be constantly tuned by its subject matter experts. Snap-on's min/max PID data, and the metadata needed to present that PID data in response to particular vehicles and symptoms, is highly proprietary and is of immeasurable competitive value to Snap-on. Plaintiffs do not share the "known good range" for the PID data with their subscribers, even on an individual vehicle basis.

70. Snap-on's and Mitchell 1's software engineers have also spent years developing custom code to manage their data and to organize data requests from products to their data servers. Invisible to the user, this software formats a user's request for certain proprietary diagnostic and repair information into a "call" or "query string" that will be recognized by the application programing interface ("API") for Plaintiffs' data servers. The query contains identifying information for the particular vehicle at issue, as well as data on the problem with the vehicle. These query strings are created by, and unique to, Snap-on and Mitchell 1 and are based on their software engineers' decisions for naming and categorization of the underlying vehicle characteristics.

71. Underlying these queries are tens of thousands of lines of code that are used to manage Plaintiffs' proprietary data and to retrieve the appropriate data to provide to end users. This code is used to organize, manage, and search over 430 million individual artifacts of data, so that a response to a query can be presented to an automotive technician almost instantaneously.

E. Snap-on's and Mitchell 1's Security Measures

72. Because the proprietary diagnostic and repair information is so important to Snap-on and Mitchell 1, they have put in place many measures to make sure it remains confidential.

73. The core commercial value of Plaintiffs' products lies in the uniquely comprehensive coverage and the broad scope of their combined data, covering

diagnostic and repair information for vehicles going back over 20 years. Thus, while end users can make individual queries in the system (subject to certain restrictions and agreements), this combined data as a whole is not accessible to them. Snap-on products do not allow users to comprehensively pull batches of information about, for example, all of the different repairs for multiple cars or multiple trouble codes.

Internal Security Measures

74. Snap-on and Mitchell 1 employees who work with their proprietary diagnostic and repair information must agree to confidentiality policies with restrictions on the use and disclosure of confidential business information and comply with confidentiality provisions expressed in various documents outlining the companies' standards. Among other things, these employees must sign a confidentiality agreement governing treatment of the proprietary and diagnostic information, technical data, trade secrets, and other confidential information.

75. Snap-on and Mitchell 1 also train their employees in the proper handling of confidential information, including the proprietary diagnostic and repair data. Each year, employees are required to complete various training modules relating to information security, cyber security, and the protection of data and intellectual property.

76. The proprietary diagnostic and repair information is stored on password-protected servers, which are accessible only by those with a need to use them. Even internal users need special access permissions to access these servers. Visitors must sign in and be escorted when they go through company facilities.

77. Snap-on and Mitchell 1 do not license their comprehensive data set to anyone.

Snap-on Handheld Diagnostic Units

78. Snap-on implements data protection measures to authenticate legitimate device usage and prevent unauthorized actors from retrieving data from

its servers. Snap-on's security process is designed to require physical possession of a Snap-on handheld diagnostic unit and the purchase of a current version bundle of software.

79. Prior to obtaining any diagnostic data from Plaintiffs' servers, each device must pass authorization and authentication challenges. Upon initiation, each diagnostic device must first authenticate by exchanging a particular set of credentials with a security server located in San Diego, California, and then it must again obtain new temporary authorization every five minutes. A device that does not pass either of these two steps cannot access Plaintiffs' data. This authentication and authorization process is implemented through over 30,000 lines of custom code written by Plaintiffs' in-house software engineers.[1]

80. In addition, the proprietary diagnostic and repair information features work only when the handheld diagnostic unit is connected to an OBD-II port and reading trouble codes. As a result, the user must either be physically connected to each vehicle subject to an information request or have built a vehicle simulator device for each vehicle, with active trouble code(s). Such simulators are not commercially available but would need to be custom built by vehicle communication engineering groups who have had access to the individual vehicles or the vehicles' controllers. As a result, it is difficult to build simulators that comprehensively address all the potential trouble codes and conditions that a specific vehicle could present.

81. Even with these layers of security in place, Snap-on still does not provide users with access to more data than is necessary to perform the repair(s) at issue. The diagnostic unit only displays information relevant to the particular trouble code(s) detected on the vehicle. Moreover, Snap-on does not display its highly proprietary PID min/max data to the user at all. Rather, the handheld

[1] This authentication and authorization process is not described in more detail here to avoid filing the Complaint under seal.

diagnostic unit identifies specific PID values that exceed the known good range turning a flag red without showing the user what that range is, as depicted in paragraph 44 above.

82. Use of Snap-on's handheld diagnostic units is also governed by a EULA that must be agreed to by the user or by a Snap-on franchisee on the user's behalf when the device is first purchased and then accepted each time the device software is upgraded. In addition, every time the user starts the diagnostic device software, a URL for the Snap-on EULA is displayed, along with a reference to the terms and conditions for use of the device. This screen states "Use of Software is governed by the terms and conditions of the End User License Agreement." A true and correct copy of this screen is attached as Exhibit 5. As described in more detail below, the Snap-on EULA prohibits, among other things, reverse engineering of the device software, running the software on multiple computers, or providing the software to a third party.

ProDemand and TruckSeries

83. All users of Mitchell 1's web-based ProDemand and TruckSeries repair information products must have an active subscription, along with user credentials tied to that subscription. To access ProDemand or TruckSeries, the user typically must have a valid username and password. For some of Mitchell 1's largest customer accounts, technicians may authenticate without a username and password by using a designated company IP address through which the customer routes their technician network traffic. The data that are transferred between the user and ProDemand or TruckSeries (and vice versa) during use of these services is encrypted through HTTPS encryption.

84. Both ProDemand and TruckSeries use an authorization process similar to the one described above for Snap-on's diagnostic units, utilizing much of the same custom-built code, which requires a new temporary authorization every five minutes in order to make a valid request for data.

85. Mitchell 1 has an anti-piracy team responsible for monitoring account access and usage and preventing misuse of its services. This team monitors server traffic for, among other things, suspicious or inconsistent IP addresses using an account, or unusual account access patterns that are indicative of unauthorized use.

86. The anti-piracy team will investigate suspicious account traffic and, if it is unable to confirm that the account is being used consistently with the EULA, will reset the account's credentials, block suspect IP addresses, or otherwise escalate the issue as appropriate.

87. Mitchell 1 account holders for both ProDemand and TruckSeries must also agree to a EULA when placing an order for an account subscription. As described in more detail below, among other things, this EULA permits usage of data only to provide vehicle repairs and estimates and conduct vehicle shop management. Further, the EULA expressly prohibits allowing the Product or data from the Product to be made available to any other person; transferring or passing along the data, the Product or access to the Product; and translating, reverse engineering, decompiling, or otherwise accessing the source codes.

F. Recent Intrusion into Snap-on's and Mitchell 1's Data Servers

88. In mid-November 2020, Snap-on began detecting unusual spikes in traffic that impacted the performance of its diagnostic device network.

89. Snap-on suspected this unusual activity was associated with illicit automated use of its diagnostic devices because legitimate users' access to Snap-on's data servers do not typically cause spikes in server traffic of this nature and because the speed at which requests were being made was faster than a human could make them. These requests were inconsistent with how Snap-on's product is normally used for repair. For example, a technician fixing a vehicle will typically look up specific service information related to the finite problems exhibited on that vehicle and the technician will linger on the material relating to that code for at least a few minutes as it is being reviewed. A technician attempting to resolve a

specific problem on a real vehicle will not systematically run through the catalog of information available for a particular make and model of a vehicle. Nor will the technician quickly look through the same information across many vehicles. This is particularly impossible for Snap-on diagnostic devices because the devices are designed to display information for only the trouble codes on the vehicle that is connected to the device. To quickly move from the trouble codes from one vehicle to those from another vehicle and then to those from another, or to a large number of trouble codes, the device would need to be rapidly connected to various vehicles.

90. Over a three-day period from November 11 to 13, 2020, Snap-on observed over *5.6 million* of such search queries seeking Plaintiffs' proprietary data. The intensity and speed of these requests is exemplified by the fact that on November 12, between the hours of 2:00 and 3:00 a.m. Pacific Time, Snap-on's IT group observed over *200,000* individual requests for data in the span of a single hour—and at a time when automotive technicians would not normally even be working in the United States. On November 13, between the same one-hour time period of 2:00 and 3:00 a.m. Pacific Time, the IT team observed over *600,000* requests.

91. As a result of this activity, legitimate customers began to complain that they were being locked out of their devices and could not access the appropriate proprietary diagnostic and repair information. This appeared to be an effect of the bad actor "spoofing" these customers' device credentials.

92. After discovering this bad actor activity, Snap-on blacklisted a set of approximately 40 IP addresses associated with the traffic and continued monitoring network traffic to block additional IP addresses engaged in suspicious activity. But, notwithstanding this blocking, the intrusions continued.

93. During the four-day period between November 21 and 25, more than *5 million additional* anomalous requests for Plaintiffs' proprietary data were made from new IP addresses that had not yet been blocked. The activity was so bad that,

to protect its data, Snap-on had to shut down access to its diagnostic servers worldwide to users of an older version of its software that was associated with the bad actor activity, cutting off access to over 15% of its legitimate customers. Periodically, over the next several weeks, during the evenings Pacific Time and on weekends, Snap-on was forced to continue shutting down access to devices using the older version of the software.

94. On or around December 7, 2020, Snap-on began generating daily reports designed to show instances where multiple devices appeared to be making requests for proprietary repair and diagnostic information through a single IP address. The daily reports reflect a significant amount of additional bad actor activity during the month of December. For example, the report for the night of December 10 through the morning of December 11 shows that at one time four different IP addresses were each making data requests, purportedly on behalf of *45* different devices *each*. This is very abnormal traffic, particularly for IP addresses coming from China, where Snap-on does not sell the ZEUS device. A report from December 12 shows that nine IP addresses in China were each making requests, purportedly on behalf of 44 devices each. A report from December 18 shows four IP addresses in China requesting data, purportedly on behalf of between 18 to 41 devices each. And a report from December 19 showed one IP address in China was purportedly making requests on behalf of 72 devices at one time, and a second IP address was purportedly making requests on behalf of another 40 devices.

95. In response to these observations, Snap-on began adding additional security mechanisms on its ZEUS devices and network, as well as additional monitoring functions to allow more detailed tracking of network activity. First, Snap-on blocked all suspected IP addresses at the firewall level. Then, on December 28, 2020, Snap-on unblocked these addresses and began sending "confused," randomized data associated with different makes and models of vehicles, rather than the actual repair and diagnostic information requested by those

IPs, and blocking unknown IP addresses from China, which was the source of much of the bad actor traffic.

96. The illicit activity still continued. Most notably, during three days in January 2021, the bad actor made over 240,000 requests for Plaintiffs' proprietary PID data. However, Plaintiffs were unable to identify the bad actor behind these activities at the time.

97. These are just examples of the illicit activity of which Plaintiffs are currently aware. Plaintiffs' investigation into the wrongful conduct is continuing.

G. Autel Gets Caught

98. The improper efforts to continue to access Plaintiffs' proprietary diagnostic and repair information continued after this time, though in lower volumes. It was these continued efforts that would eventually tip off Snap-on and Mitchell 1 that the activity was coming from Autel. In the middle of May 2021, after noticing additional suspicious activity, Plaintiffs hired outside counsel, who retained an independent forensic expert.

Snap-on Handheld Diagnostic Units

99. The expert has prepared a declaration that is being filed in support of Plaintiffs' motion for a temporary restraining order and order to show cause. That declaration reports that there are numerous links between Autel and the attack on Plaintiffs' proprietary data.

100. For example, between December 29, 2020 and July 3, 2021, at least eight different ZEUS device serial numbers were used to connect to the Plaintiffs' Authentication API from the main static IP address associated with Autel US's ProDemand account (discussed below). Seven of these devices have been used with a total of 86 IP addresses to obtain Plaintiffs' proprietary data, including IP addresses from China that were associated with the bad actor activity.

101. Plaintiffs' logs show that Autel US and Autel ITC were working in parallel to steal Plaintiffs' data, making many requests during the same time

periods, and that they were coordinated. On one notable occasion, Autel US and Autel ITC made identical requests for the same car and problem code within one minute of each other from Autel US's IP address and from an IP address in China. At that time, the Chinese IP address was being sent confused data, while the Autel US IP address was not, and Defendants were likely comparing the data that each one was receiving.

102. Autel has continued requesting Plaintiffs' proprietary data by spoofing devices throughout this time period, including as late as July 15, 2021.

103. Plaintiffs have no record of Autel ever purchasing even one of Snap-on's handheld diagnostic units, or purchasing or paying for a software upgrade to one of those units.

104. Autel has "spoofed" over 400 devices to request data from Plaintiffs' data servers, presenting the requests as coming from legitimate devices by using their serial numbers. Many of these serial numbers were authenticated and activated on the days of November 9 and 14, 2020. On November 9—right before the mass attack on Plaintiffs' servers that took place from November 11 to 13—a bad actor sequentially activated over 400 device serial numbers. These activation requests were extremely unusual both because of their high volume and their speed.

105. Then, on November 14, the day after Plaintiffs had blocked traffic to the bad actor IP addresses associated with the barrage of requests that took place from November 11 to 13, the same pattern was repeated, and over 600 device serial numbers were authenticated and activated on November 14, again in a highly abnormal, rapid-fire sequential order.

106. Of these over 1,000 devices that were activated due to these November requests, at least 276 devices were associated with high-volume anomalous data requests.

ProDemand

107. Autel US has maintained a ProDemand account since a large national customer of Mitchell 1 requested that Autel be provided with an account. The account was to be used by Autel to confirm whether its customer could access its ProDemand subscription with Mitchell 1 on the Autel devices purchased by the customer. Autel ITC has never had an account to ProDemand.

108. Plaintiffs' logs show that Autel US has been using the account in breach of the license terms of the Mitchell 1 EULA and has evidently shared its password with Autel ITC. Since at least October 1, 2020, both Autel US and Autel ITC have been systematically obtaining data from ProDemand relating to different features. Together they have made at least 9,600 search actions. Over 4,000 of those search actions have targeted ADAS features. These requests have been so extensive that Autel has made the second-highest number of requests for ADAS data of any of Plaintiffs' customers during this time period—far exceeding the number of requests even by national automobile chains with dozens of ProDemand users in multiple locations throughout the country.

109. Defendants' efforts escalated during the first two weeks of July 2021, and they continued to request this data until Mitchell 1 shut down Defendants' account on July 14, 2021, which took effect July 15, 2021.

TruckSeries

110. Neither Autel US nor Autel ITC has an account to TruckSeries, which requires a separate account and subscription from ProDemand. Nonetheless, it appears that they have been obtaining Plaintiffs' proprietary data from TruckSeries as well, through an account issued to another company, Tom Machine Equipment & Repair ("Tom Machine").

111. Autel's US IP address has been used to sign into the Tom Machine account to make requests for data. In addition, two other IP addresses have been used by both the Autel US IP account and the Tom Machine account. These were

the only three IP addresses that have been used to sign into the Tom Machine account since October 1, 2020.

112. Other factors point to Autel using the Tom Machine account as a front to obtain Plaintiffs' proprietary medium and heavy truck data. Every TruckSeries and ProDemand account has a "ship to," "bill to," and "tech account(s)" associated with it, which contain information that Plaintiffs use to communicate with and bill their customers. The customer-provided email address for the technician account associated with Autel's ProDemand account is the same as the billing email address provided by the Tom Machine TruckSeries account. The individual listed as the billing contact for the Tom Machine account is identified as an Autel consultant on the International Automotive Technicians Network website and in his blog online.

113. Since October 1, 2020, at least 800 search actions for Plaintiffs' proprietary diagnostic and repair truck information have been made through the Tom Machine account. And just between July 7 and July 12, 2021, over 470 print requests were made for that account.

H. Autel's Competing Diagnostic Devices Recently Introduced an "Intelligent Diagnostics" Feature

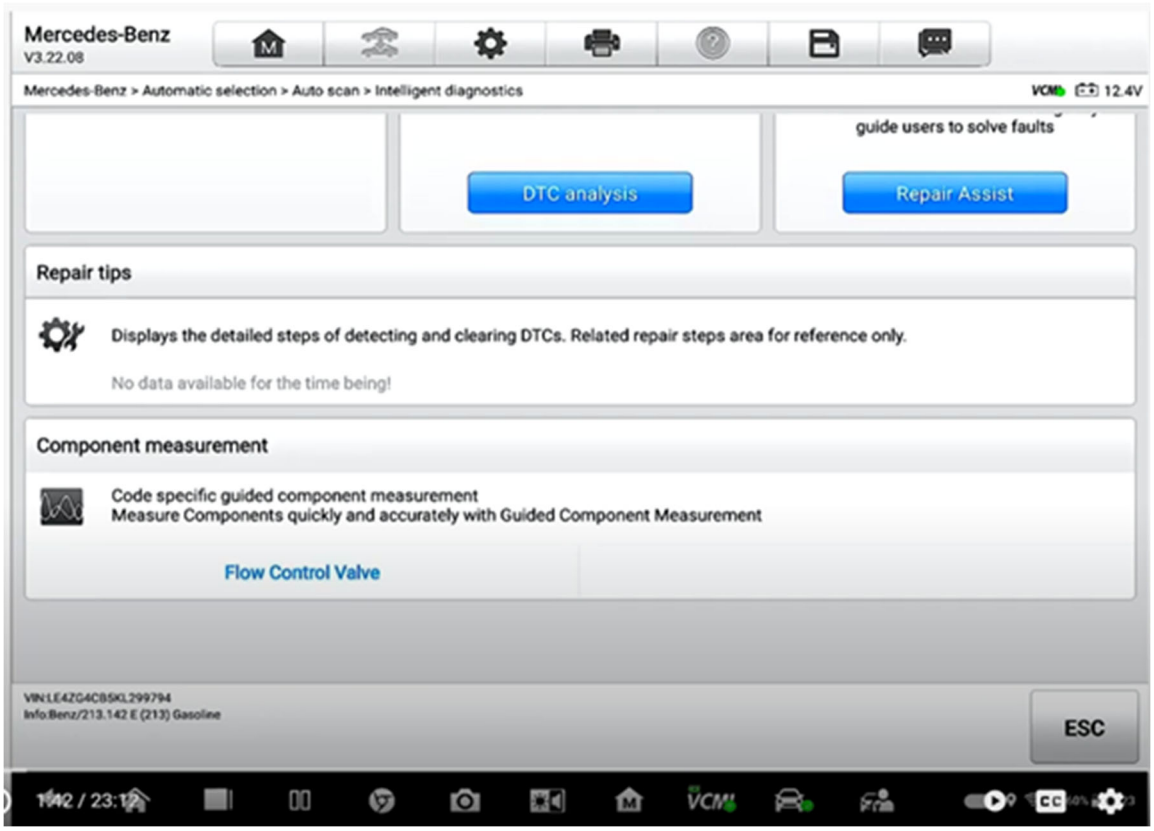
114. Autel sells diagnostic device products that compete directly with Plaintiffs' products, including its recently released MaxiSys Ultra device, which Autel describes as its "most ambitious diagnostics tablet designed to maximize technician intelligence." *See* https://www.autel.com/c/www/mk3/3525.jhtml.

115. The MaxiSys Ultra device purportedly includes an "intelligent diagnostics" feature. This feature is explained in an Autel Global video released on January 22, 2021 titled "Autel MaxiSys Ultra: How to use intelligent diagnostics" and available at https://www.youtube.com/watch?v=9LKtVq5Kwlg.

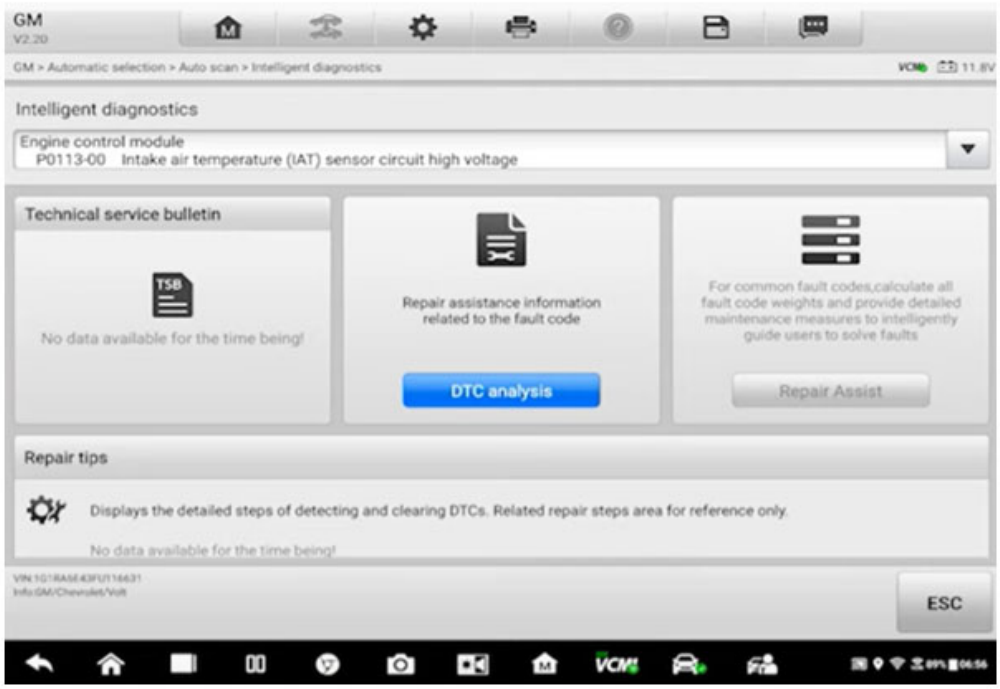
116. The Autel intelligent diagnostics feature purports to provide many of the same categories of diagnostic and repair information as Snap-on and Mitchell 1's products. The Autel tutorial video linked above explains that

intelligence diagnostics "provides diagnostic solutions to help you fix vehicles with its step-by-step guidance." Upon accessing the intelligent diagnostics interface, a user is shown different cards titled "Technical service bulletin," "DTC analysis," "Repair assist," "Repair tips," and "Component measurement." The video describes the types of information each of these cards should display. For example, the "Repair assist" card is intended to "integrate diagnostic devices, wiring diagrams, and measurement tools into one, guiding you to find reasons and solutions step by step."

117. However, while it purports to provide similar diagnostic and repair information, Autel does not have the depth of proprietary data that Snap-on and Mitchell 1 have obtained from their analysis of the billions of repair records that they uniquely possess. Even in the demonstration video that Autel has prepared, it is apparent that its device is missing data. For example, in the intelligent diagnostics interface shown in this tutorial video, there is no data underlying the "Repair tips" card for the car being demonstrated:



118. Similarly, in another tutorial released by Autel for the MaxiSys Ultra device, there is no data for the "Technical Service Bulletin" card, the "Repair assist" card, or the "Repair tips" card on the intelligent diagnostics interface:



119. As shown above, the MaxiSys Ultra already has the structure to make use of Plaintiffs' proprietary diagnostic and repair information, and the comprehensive set of data that Plaintiffs pay significant fees to license from OEMs. That data is of great value to Autel, because this data could allow Autel to both fill in the many data points it is missing and determine the accuracy of the data it has provided. Autel simply cannot obtain the same level of comprehensive data as Snap-on and Mitchell 1 because it does not have access to the billions of repair orders that Snap-on and Mitchell 1 do, and even if it did, it would have to spend years organizing and analyzing the data as Snap-on and Mitchell 1 have done. This provides Snap-on and Mitchell 1 with a unique competitive advantage in the market and years of lead time over Autel. Snap-on and Mitchell 1 will be irreparably harmed if Autel is permitted to use their data to compete against them or if Autel discloses their data to third parties.

120. Further, while the MaxiSys Ultra provides information relating to automobiles, Autel has recently expanded its products in the truck market as well.

In addition, on May 17, 2021, Autel announced that it has "introduced a diagnostic tablet for commercial vehicles, which is compatible with more than 80 models of light- medium- and heavy-duty vehicles," the MaxiSys MS909CV. *See* https://www.truckinginfo.com/10143412/autel-adds-commercial-vehicle-diagnostics-tablet. Snap-on and Mitchell 1 have spent years compiling and developing the repair and diagnostic information contained in TruckSeries, which has been authored by them to provide a uniquely detailed and comprehensive set of data for medium and heavy truck repair. Snap-on and Mitchell 1 will be irreparably harmed if Autel were to disclose this data or use it in its own diagnostic truck product.

FIRST CAUSE OF ACTION

DMCA - Circumvention of Security Measures under 17 U.S.C. § 1201
(Against Both Defendants)

121. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 as if fully set forth herein.

122. Autel US and Autel ITC have each violated the DMCA, 17 U.S.C. § 1201(a)(1)(A), by unauthorized circumvention of technological measures for Plaintiffs' handheld diagnostic computers that control access to Plaintiffs' databases of proprietary diagnostic and repair information and associated software protected by the Copyright Act.

123. As described in more detail above, Plaintiffs have implemented numerous technological measures which control access to their diagnostic and repair information and the associated data services software used to manage it. For example, Snap-on implements an authentication and authorization process that is designed to require possession of a Snap-on handheld diagnostic device and the appropriate version of associated software in order to access Snap-on's proprietary diagnostic and repair information, and the software that manages that data. Snap-on made extensive efforts to create this security software, which consists of more

than 30,000 lines of code and took two to three software developers three years to implement, working nearly full time. Among other things, this process requires two pieces of unique device identifying information that must be authenticated. A device that passes the authentication process must then obtain new temporary authorization every five minutes. A device that does not pass these authentication and authorization steps cannot access either Snap-on's proprietary diagnostic and repair information or the data server software that manages it and returns the data. Therefore, this process is a technological measure that controls access to Snap-on's proprietary diagnostic and repair information and associated software.

124. Additionally, to gain access to Snap-on's proprietary diagnostic and repair information, the diagnostic device must be connected to a vehicle's OBD-II port and reading trouble codes. This means that a user must physically connect their device to a vehicle or have built a vehicle emulator for the device, which would have to be custom made. And, even when a device is connected to a vehicle, the diagnostic and repair information presented via the device's software is limited to information that corresponds to the year/make/model/engine of the vehicle and the particular repair at issue. Therefore, these technological measures also control access to aspects of Snap-on's proprietary data.

125. As described above, Autel US and Autel ITC have each engaged in unauthorized circumvention of Snap-on's above-described technological processes to "spoof" multiple devices, presenting the wrongfully obtained credentials of hundreds of devices to authenticate those devices, and then obtaining the required authorization for each device and regularly refreshing that authorization, thereby obtaining access to Snap-on's proprietary diagnostic and repair data contained on Plaintiffs' servers and the software used to manage it and to search for and return the data in response to requests. Further, rather than obtaining data only for vehicles that were connected to the diagnostic device, Autel US and Autel ITC made use of an automated process to systematically make requests directly for

vehicle makes and models that it never connected to the devices, thereby circumventing Plaintiffs' technological measures to protect its compilation of proprietary data.

126. This proprietary diagnostic and repair data and its associated software comprise "works" subject to copyright protection under 17 U.S.C. § 102. The proprietary diagnostic and repair information provided by this software (e.g., Real Fixes, Smart Data) was created, compiled, and organized by Plaintiffs based on a combination of many years of compiling real world data, expert analysis of that data, and artificial intelligence software. In addition to all of the unique data points that were determined based on this analysis, the proprietary diagnostic and repair information includes literally millions of original narrative descriptions, all of which are uniquely created, arranged, and organized by Plaintiffs. Moreover, Plaintiffs built a comprehensive taxonomy and ontology to organize diagnostic and repair terminologies across all vehicle makes, models, and engine systems in the databases. Thus, Plaintiffs' proprietary diagnostic and repair data comprises "works" subject to copyright protection due to both (1) the original content included in this data and (2) the original data compilation as a whole. Further, the data services software created for managing and returning data from Plaintiffs' massive databases of information is original source code that was created in-house over a period of years, that easily amounts to tens of thousands of lines of code or more, and that took eight to ten person-years to create. Many original design choices were made in the course of creating this code, and it is thus protected as an original literary work.

127. Autel US and Autel ITC have each further violated section 1201(a)(1)(A) of the DMCA via their unauthorized circumvention of technological measures that control access to Mitchell 1's TruckSeries product and the data services software that manages it.

128. Mitchell 1 has implemented technological measures which control access to its web-based proprietary TruckSeries product. As described above, access to the TruckSeries product requires users to purchase a monthly subscription, and to create a user name, and password (or in the case of certain larger customers, authentication through use of a specific, designated IP address). A user who does not meet these requirements and possess an active subscription cannot access TruckSeries. Further, TruckSeries uses an authorization process similar to the one described above for Snap-on's diagnostic units, utilizing much of the same custom-built code, which requires a new temporary authorization every five minutes in order to make a valid request for data. A request that is unauthorized cannot access the TruckSeries data or data services software.

129. The TruckSeries product provides diagnostic and troubleshooting information for medium and heavy duty trucks. It is an original work of authorship comprising a unique compilation of proprietary content. The TruckSeries web program and the proprietary content within are "works" subject to copyright protection under 17 U.S.C. § 102. The content is authored by Plaintiffs and is copyright protected. It includes, among other things, high resolution photographs and CAD drawings created by Mitchell 1 that have been highlighted, color-coded, and labeled, interactive original wiring diagrams, labor estimates for how much time Snap-on's experts believe a repair should take, ADAS reference tables, written narratives, and more, all uniquely arranged and organized. In addition to the copyright protection afforded to these original works, the proprietary content provided by this software was compiled and organized by Mitchell 1 and is therefore protected at least as an original data compilation. The TruckSeries product utilizes the same data services software described above, that was created in-house over a period of several years and is thus protected as an original literary work.

130. Neither Autel US nor Autel ITC has a registered account to TruckSeries. Neither Autel US nor Autel ITC has a legitimate username or

password. They have circumvented the technological measures that control access to Plaintiffs' TruckSeries product by accessing TruckSeries and its proprietary content using an account registered to another company, Tom Machine, and presenting their data queries as though they were authorized queries coming from a legitimate authenticated account.

131. The Mitchell 1 EULA that applies to TruckSeries (as well as ProDemand) provides that "Customer may not . . . allow the Product or data from the Product to be made available to any person other than Customer" or "assign, sell, transfer or pass along the data, the Product or access to the Product." Exhibit 2 at 75 (¶ 4(b)).

132. In addition to their individual violations, Autel US and Autel ITC conspired with one another to breach 17 U.S.C. § 1201(a)(1)(A) with respect to Snap-on's handheld diagnostic devices and the TruckSeries account through the conduct described above. Autel US and Autel ITC agreed to work together to circumvent the technological measures designed to control access to Plaintiffs' databases of proprietary diagnostic and repair information and associated software for these two products that are protected by the Copyright Act, and gained improper access to this information and software from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted behavior, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main, static Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful acts described above.

133. In addition, Autel ITC has violated section 1201(a)(1)(A) of the DMCA via its unauthorized circumvention of technological measures that control access to Mitchell 1's ProDemand product.

134. Access to the ProDemand product is protected by the same technological measures which control access to Mitchell 1's web-based proprietary TruckSeries product, including the authentication and authorization processes described above and the requirement for a subscription account with a user name and password. Autel ITC does not have a subscription to ProDemand and does not have a legitimate user name or password to an account. Autel ITC circumvented the technological measures designed to protect access to ProDemand accounts by using the account, user name, and password of Autel US, and presenting its data queries as though they were authorized queries coming from the Autel US account.

135. ProDemand is an original work of authorship comprising a unique compilation of proprietary content and OEM content, much of which is licensed at a substantial fee. The ProDemand web program and the proprietary content within are "works" subject to copyright protection under 17 U.S.C. § 102. The proprietary content included in ProDemand that is authored by Plaintiffs includes the millions of Real Fix narratives, the TroubleShooter narratives, Top Repairs, and Top 10 Repairs, as described above; this proprietary content comprises protected original works. In addition to the copyright protection afforded to these original works, the proprietary content provided by this software was compiled and organized by Mitchell 1 in a unique fashion and is therefore protected at least as an original data compilation. The ProDemand product utilizes the same data services software described above, that was created in-house over a period of several years, includes tens of thousands of lines of code, and is protected as an original literary work.

136. Plaintiffs have been damaged by Autel's above-described circumvention of various technological measures that control access to their various copyrighted works in an amount to be proven at trial.

137. Autel's above-described conduct has caused and, unless enjoined, will continue to cause, irreparable harm to Plaintiffs.

138. As a result of Autel's unlawful circumvention, Plaintiffs are entitled to an injunction, actual damages and any additional profits of Defendants pursuant to 17 U.S.C. § 1203(c)(2) or statutory damages pursuant to 17 U.S.C. § 1203(c)(3). Plaintiffs are further entitled to costs, including reasonable attorney's fees pursuant to 17 U.S.C. § 1203(b).

SECOND CAUSE OF ACTION

Violation of CFAA under 18 U.S.C. § 1030(a) (Against Both Defendants)

139. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 as if fully set forth herein.

140. Defendants have acted individually and conspired with one another to violate various provisions of the CFAA.

141. Snap-on's handheld diagnostic computers are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2). Plaintiffs' servers, computers, computer systems, and computer networks that support the functionality of their diagnostic systems and related subscription services (e.g., ProDemand and TruckSeries) are also "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2).

142. Defendants have each individually violated the CFAA, 18 U.S.C. § 1030(a)(5)(C), by intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage and loss to Plaintiffs.

143. As set forth in more detail above, Autel US and Autel ITC each circumvented the technical measures designed to protect Plaintiffs' protected computers, and then "spoofed" those devices to present authorization credentials in order to access the proprietary vehicle diagnostic and repair data that are stored on

Plaintiffs' servers. Autel had no authorization to access these protected computers and obtain this data.

144. In addition, Autel had no authorization to access and use the TruckSeries product. Neither Autel US nor Autel ITC have a paid subscription, user name, or password to TruckSeries, but each has used the user name and password issued to Tom Machine to access the TruckSeries product and the proprietary diagnostic and repair information for medium and heavy trucks that are stored on Plaintiffs' servers. Autel US and Autel ITC had no authorization to access these protected computers and obtain this data.

145. These same facts evidence a violation of 18 U.S.C. section 1030(a)(4) of the CFAA. Autel US and Autel ITC each knowingly, and with the intent to defraud Plaintiffs, accessed a protected computer, without authorization or by exceeding authorized access to such a computer, and by means of such conduct furthered the intended fraud and obtained one or more things of value, including but not limited to Plaintiffs' proprietary data.

146. As described above, Autel US and Autel ITC both fraudulently spoofed Snap-on's handheld diagnostic computers to access proprietary vehicle diagnostic and repair information stored on Plaintiffs' servers, when they had no authorization to do so, disguising the requests so that they appeared to be coming from legitimate devices when in fact they were not and were coming from Defendants.

147. Similarly, Autel US and Autel ITC fraudulently presented the user name and password assigned to Tom Machine to obtain access to TruckSeries and proprietary diagnostic and repair information relating to medium and heavy trucks from Plaintiffs' servers.

148. In addition to their individual violations, Autel US and Autel ITC conspired with one another to breach 18 U.S.C. sections 1030(a)(4) and 1030(a)(5)(C) with respect to Snap-on's handheld diagnostic devices and the

TruckSeries account through the conduct described above. Autel US and Autel ITC agreed to work together to siphon the proprietary data from the data servers associated with these two products, and gained improper access to these data servers from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted behavior, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main, static Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful acts described above.

149. In addition, Autel ITC violated sections 1030(a)(4) and 1030(a)(5)(C) of the CFAA, by knowingly and with the intent to defraud Plaintiffs, utilized the user name and password assigned to Autel US for Mitchell 1's ProDemand service to obtain access to at least the OEM licensed data stored on Plaintiffs' protected data servers. Autel ITC does not have a ProDemand account, and was not authorized by Plaintiffs to use ProDemand. Via its use of ProDemand, knowingly and with the intend to defraud Plaintiffs, Autel ITC accessed a protected computer, without authorization, and by means of such conduct furthered the intended fraud and obtained one or more things of value, violating section 1030(a)(4) of the CFAA. This conduct also violated section 1030(a)(5)(C) of the CFAA because Autel ITC intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs.

150. As a result of Autel's conduct, Plaintiffs have suffered damage and loss in an amount to be proven at trial but, in any event, in an amount far in excess of $5,000 aggregated over a one-year period as provided for in 18 U.S.C. § 1030(a)(4). Among other things, Plaintiffs have been forced to spend a substantial

amount of money to respond to Autel's conduct, and their service to customers was interrupted and impaired multiple times, as set forth in more detail above.

151. Autel's unlawful access to and theft from Plaintiffs' computers has caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Remedies at law are not adequate to fully compensate Plaintiffs for these injuries, entitling Plaintiffs to injunctive relief as provided by 18 U.S.C. § 1030(g).

THIRD CAUSE OF ACTION

Violation of California's Computer Data Access and Fraud Act under Cal. Penal Code § 502(c))
(Against Both Defendants)

152. Plaintiffs restate and incorporate by reference all foregoing Paragraphs 1 through 120 and 139 through 151 as if fully set forth herein.

153. Defendants have acted individually and conspired with one another to violate various provisions of California's Computer Data Access and Fraud Act (Cal. Penal Code § 502(c)).

154. Defendants have each individually violated California Penal Code section 502(c)(7) by knowingly and without permission accessing Plaintiffs' computer, computer system, or computer network.

155. As described in detail above, Autel US and Autel ITC, each knowingly and without permission accessed the proprietary diagnostic and repair information located on Plaintiffs' data servers by spoofing Snap-on's handheld diagnostic computers, disguising the requests as having come from legitimate devices to pass the authentication protocol and gain access to the data servers. Autel US and Autel ITC were fully aware that they had not purchased these spoofed devices and that they had never purchased subscriptions for the devices, and that they had no permission to use the identifying information for the devices to request information.

156. In addition, Autel US and Autel ITC, each knowingly and without permission, made use of the user name and password issued to Tom Machine to

gain access to the TruckSeries product and to Plaintiffs' computer network to access the proprietary diagnostic and repair information relating to medium and heavy trucks on Plaintiffs' data servers. Again, Autel US and Autel ITC were fully aware that they were not the registered users of the account and had no right to make use of the user name and password to obtain this data.

157. Further, defendant Autel ITC, knowingly and without permission, made use of the user name and password issued to Autel US to gain access to the ProDemand product and to Plaintiffs' computer network to access the repair information contained on Plaintiffs' data servers associated with that product. Autel ITC was fully aware that it did not possess an account for the ProDemand product, but made use of the Autel US account anyway. Further, although Autel US did have a user name and password for ProDemand, it violated California Penal Code section 502(c)(7) by knowingly logging into ProDemand and accessing and taking and using information from ProDemand and Plaintiffs data servers improperly. Autel US's actions in siphoning Plaintiffs' data to compete against Plaintiffs exceeded the permitted uses under the terms of the ProDemand EULA to which it agreed, which were: (i) providing vehicle mechanical services; (ii) estimating vehicle mechanical parts and labor cost estimates; and (iii) conducting vehicle shop management. Exhibit 2 at 75 (¶ 4(a)); Exhibit 4 at 82 (¶ 4). Autel US's actions were also prohibited by the ProDemand EULA, which among other things, provides that an End User may not (i) copy or reproduce the Product except as permitted in this Agreement; or (ii) allow the Product or data from the Product to be made available to any person other than End User. Exhibit 2 at 75 (¶ 4(b)). By providing its password to Autel ITC, Autel US made the data from ProDemand available to Autel ITC, fully aware that it was violating the permitted uses of its account, which were set forth in the EULA to which it had agreed.

158. These facts above also constitute a violation of California Penal Code section 502(c)(1), by both Autel US and Autel ITC with respect to Snap-on's

handheld diagnostic tools, the TruckSeries product, and the ProDemand product because Autel knowingly accessed, and without permission used Plaintiffs' data, computer, computer system, or computer network in order to wrongfully control or obtain Plaintiffs' data.

159. In addition Autel US and Autel ITC have each violated California. Penal Code section 502(c)(5) by knowingly and without permission causing the disruption of computer services and causing the denial of computer services to authorized users of Plaintiffs' computers, computer system, or computer network. Autel US and Autel ITC knew that they did not have permission to access the proprietary data accessible through Snap-on's diagnostic devices as they were not paying a subscription fee for the devices and were making use of the credentials of devices that they had never purchased or registered. Autel US and Autel ITC knew that this would severely impact Plaintiffs' network. They deliberately bombarded Plaintiffs' network and data servers with hundreds of thousands or millions of requests over compressed time periods, at times spoofing dozens of devices from a single IP address to carry out their raid on Plaintiffs' data. Autel US and Autel ITC knew that their use of these spoofed credentials and the extreme amount of traffic that they were sending to Plaintiffs' network from multiple IP addresses and devices would interfere with Plaintiffs' network and its ability to provide services to legitimate customers and other authorized users of this network.

160. As described in more detail above, as a result of Autel US and Autel ITC each knowingly and without permission spoofing multiple handheld diagnostic computers, and extensively attacking Plaintiffs' data servers, service to Plaintiffs' customers was cut off or interrupted, and Plaintiffs were forced to shut down worldwide access to customers on their data servers on multiple occasions.

161. In addition to their individual violations, Autel US and Autel ITC conspired to violate California Penal Code sections 502(c)(1), and 502(c)(7) with respect to Snap-on's handheld diagnostic devices and the TruckSeries account

through the conduct described above. Autel US and Autel ITC conspired, agreed, and had a common plan and design to work together to siphon the proprietary data from the data servers associated with these two products, and gained improper access to these data servers from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted activity, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful acts described above.

162. Further, Autel US conspired and agreed, and had a common plan and design, to enable Autel ITC to clandestinely obtain access to ProDemand and to take ProDemand data from Plaintiffs' servers. They agreed to share Autel US's user name and password, so that this information could be obtained by Autel ITC without Plaintiffs' knowledge—even though they knew that Autel ITC had no permission to access this information—to coordinate to systematically take data from ProDemand in violation of the uses permitted by the EULA. This agreement is further evidenced by the parallel taking of ProDemand data from Plaintiffs' servers by Autel US and Autel ITC. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful acts described above.

163. As a result of Autel's violations of this Act, Plaintiffs are entitled to compensatory damages for the harm caused by their actions, and to injunctive relief. Autel's violations of this Act have caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Remedies at law are not adequate to fully compensate Plaintiffs for these injuries,

entitling Plaintiffs to injunctive relief as provided by California Penal Code section 502(e)(1).

FOURTH CAUSE OF ACTION

Violations of Wisconsin Computer Crimes Act under Wis. Stat. § 943.70
(Against both Defendants)

164. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 and 139 through 151 as if fully set forth herein.

165. As an alternative to the Third Cause of Action above, for the violation of California Penal Code section 502(c), should the Court find that Wisconsin statutory law applies to Autel's conduct relating to the handheld diagnostic computers, Defendants are both liable for individually violating the Wisconsin Computer Crimes Act, set forth in Wisconsin Statute section 943.70, and for conspiring with one another to violate the Act.

166. If the Wisconsin Computer Crimes Act applies, Autel US and Autel ITC have each individually violated multiple sections of that statute.

167. Autel US and Autel ITC each violated Wisconsin Statute section 943.70(2)(a)(3) because they knowingly and without authorization accessed Snap-on's computer programs or supporting documentation. As described in detail above, Autel US and Autel ITC knowingly and without authorization accessed computer programs relating to Snap-on's handheld diagnostic computers, the TruckSeries product, and the data servers containing Plaintiffs' proprietary data associated with each of those products. Further, Autel ITC knowingly and without authorization accessed computer programs relating to the ProDemand product.

168. Autel US and Autel ITC, each knowingly and without permission accessed the proprietary diagnostic and repair information located on Plaintiffs' data servers by spoofing Snap-on's handheld diagnostic computers, disguising the requests as having come from legitimate devices to pass the authentication protocol and gain access to the data servers. Autel US and Autel ITC were fully aware that

they had not purchased these spoofed devices and that they had never purchased subscriptions for the devices, and that they had no permission to use the identifying information for the devices to request information.

169. In addition, Autel US and Autel ITC, each knowingly and without permission, made use of the user name and password issued to Tom Machine to gain access to the TruckSeries product and to Plaintiffs' computer network to access the proprietary diagnostic and repair information relating to medium and heavy trucks on Plaintiffs' data servers. Again, Autel US and Autel ITC were fully aware that they were not the registered users of the account and had no right to make use of the user name and password to obtain this data.

170. Further, defendant Autel ITC, knowingly and without permission, made use of the user name and password issued to Autel US to gain access to the ProDemand product and to Plaintiffs' computer network to access the repair information contained on Plaintiffs' data servers associated with that product. Autel ITC was fully aware that it did not possess an account for the ProDemand product, but made use of the Autel US account anyway.

171. Autel US and Autel ITC each further violated Wisconsin Statute sections 943.70(2)(a)(4) and (a)(5) because they knowingly and without authorization took possession of and copied Plaintiffs' data. As described above, Autel US and Autel ITC knowingly and without authorization each obtained from Plaintiffs' data servers the proprietary diagnostic and repair information associated with Snap-on's handheld diagnostic computer and the TruckSeries products. Further, Autel ITC knowingly and without authorization accessed ProDemand and obtained from Plaintiffs' data servers the repair information associated with the ProDemand product. Therefore, Autel US and Autel ITC knowingly possessed, copied, and likely still possess, Snap-on's diagnostic and repair information that they were, and are, not authorized to possess.

172. In addition, Autel US and Autel ITC conspired with one another to breach Wisconsin Statute sections 943.70(2)(a)(3), 943.70(2)(a)(4), and 943.70(2)(a)(5) with respect to Snap-on's handheld diagnostic devices and the TruckSeries account through the conduct described above. Autel US and Autel ITC conspired, agreed, and had a common plan and design, to work together to siphon the proprietary data from the data servers associated with these two products, and gained improper access to these data servers from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted activity, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful conduct described above.

173. In addition, Autel US violated Wisconsin Statute § 943.70(2)(a)(6) by disclosing restricted access information to an unauthorized entity, Autel ITC, because it disclosed its user name and password to Autel ITC, enabling Autel ITC to access ProDemand data from Plaintiffs' data servers. Further, Autel US and Autel ITC conspired and agreed, and had a common plan and design, in violation of Wisconsin Statute section 943.70(2)(a)(6), by agreeing to provide the user name and password of Autel US to Autel ITC to enable Autel ITC to clandestinely obtain access to ProDemand and to take ProDemand data from Plaintiffs' servers without Plaintiffs' knowledge—even though they knew that Autel ITC had no permission to access this data. This agreement is further evidenced by the parallel taking of ProDemand data from Plaintiffs' servers by Autel US and Autel ITC. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful conduct described above.

174. Autel's violations of the Wisconsin Computer Crimes Act have caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Remedies at law are not adequate to compensate Plaintiffs for these injuries. Plaintiffs are therefore entitled to injunctive relief under Wisconsin Statute section 943.70(5).

FIFTH CAUSE OF ACTION

Breach of Contract under the Snap-on End User License Agreement
(Against both Defendants)

175. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 as if fully set forth herein.

176. Users of Snap-on's diagnostic devices and services are subject to an End User License Agreement ("Snap-on EULA"). A true and correct copy of this agreement is attached as Exhibit 6.

177. Snap-on products are generally sold via a distribution model. Snap-on franchisees or Snap-on employees will sell the ZEUS diagnostic device directly to end user technicians or shops. Generally, the franchisee selling a diagnostic tool will explain and/or present the EULA to the customer, and will agree to the EULA on their behalf. Future software updates also require acceptance of the EULA. Because software bundles expire, and the device authentication requires a software bundle version within the current range, users must agree to the EULA to maintain their access to Snap-on's servers. Additionally, every time a user opens a Snap-on diagnostic device's software, a screen with a URL to the Snap-on EULA is provided.

178. The Snap-on EULA delineates the following permitted and prohibited uses of Snap-on's diagnostic software:

> **PERMITTED USES** YOU MAY: (i) install the Software on a single automotive diagnostic computer, the diagnostics tool for which it was intended, provided you keep the original solely for backup or archival purposes; (ii) transfer the Software and License to another party if

> the other party agrees to accept the terms and conditions of this Agreement, you retain no copies of the Software, and you transfer all of the Software to such other party. Exhibit 6 at 87.
>
> **PROHIBITED USES** YOU MAY NOT: (i) copy the Software into any machine readable or printed form for backup or archival purposes; (ii) modify, merge, translate, decompile, reverse engineer, disassemble, decode, or otherwise alter or attempt to derive the source code of the Software; (iii) use the Software on more than one computer at the same time; (iv) separate the Software's component parts for use on more than one computer; the diagnostics tool for which it was intended (v) transfer, assign, rent, lease, sell, or otherwise dispose of the Software on temporary or permanent basis except as expressly provided herein; (vi) use the Software in any outsourcing, timesharing or service bureau arrangement; and/or (vii) provide, disclose, divulge or make available to, or permit use of the Software by any third party without Snap-on's prior written consent. You will not remove any proprietary notices from the Software and will include such notices on any authorized copies of the Software. Exhibit 6 at 87.

179. The Snap-on EULA is a valid contract.

180. Autel agreed to the terms of the EULA when it made use of Snap-on's diagnostic device software, and when it upgraded the device software. Autel has made requests for Plaintiffs' proprietary data on at least software versions 20.2, 20.4 and 21.2.

181. Plaintiff Snap-on has complied with all of the conditions and obligations of the Snap-on EULA.

182. Upon information and belief, Autel has breached the Snap-on EULA by both exceeding the delineated "permitted uses" and engaging in the "prohibited uses" of Snap-on's diagnostic software.

183. Autel exceeded the Snap-on EULA's "permitted uses" of Snap-on's software, and engaged in prohibited uses when it made use of the software to spoof multiple devices at the same time to scrape large amounts of proprietary data, when it separated the software's component parts to spoof multiple devices at one time and, on information and belief, when it reverse engineered or otherwise derived

source code from the software that allowed it to satisfy the authentication and authorization protocol for the devices and to access the data contained on Plaintiffs' data servers; and when it reverse engineered or otherwise derived source code from the software that allowed it to formulate properly structured and authorized queries requesting data. This use goes far beyond the Snap-on EULA's permitted use of "install[ing] the Software on a single automotive diagnostic computer, the diagnostics tool for which it was intended." Exhibit 6 at 87.

184. As a result of Autel's actions, Plaintiff Snap-on has been damaged in an amount to be proven at trial, and is entitled to recover damages to fully compensate for that harm.

185. In addition Autel's violations of this agreement have caused Snap-on irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Remedies at law are not adequate to fully compensate Snap-on for these injuries, entitling Snap-on to injunctive relief.

SIXTH CAUSE OF ACTION

(Breach of Contract under the Mitchell 1 End User License Agreement)
(Against Defendant Autel US only)

186. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 as if fully set forth herein.

187. As discussed above, Autel US signed the Mitchell 1 EULA when it opened a ProDemand account on or around January 25, 2016. A true and correct copy of Autel US's order form and EULA signature page is attached as Exhibit 1. A true and correct copy of Mitchell 1's 2016 EULA (which is more legible and more complete than the EULA signature page) is attached as Exhibit 2. Autel US has maintained this account to ProDemand. In December 2020, Autel US signed an order form for ProDemand adding five users to its license, in which it confirmed its earlier agreement to the EULA. A true and correct copy of the order form that was signed by Autel US in 2020 is attached as Exhibit 3, and a true and correct copy of

the Order Terms and Conditions that accompanied that order form is attached as Exhibit 4.

188. The 2016 and 2020 Mitchell 1 EULAs are valid agreements. Plaintiff Mitchell 1 has complied with all of the conditions and obligations of the 2016 Mitchell 1 EULA and 2020 Mitchell 1 Order Terms and Conditions.

189. The 2016 Mitchell 1 EULA and 2020 Mitchell 1 Order Terms and Conditions specify that the licensed use of ProDemand is solely for certain purposes. The permitted uses delineated in the 2016 Mitchell 1 EULA and 2020 Mitchell 1 Order Terms and Conditions include:

> "(i) providing vehicle mechanical services; (ii) estimating vehicle mechanical parts and labor cost estimates; and (iii) conducting vehicle shop management. Unless the Order Form specifies otherwise, the license shall be for one location; with location referring to a distinct building or site. If the Order Form authorizes more than one user, then the number of users shall be limited to the number set forth on the Order Form." Exhibit 2 at 75 (¶ 4(a)); Exhibit 4 at 82-83 (¶ 4).

190. The prohibited uses described in the 2016 Mitchell 1 EULA provides that:

> Customer may not (i) copy or reproduce the Product except as permitted in this Agreement; (ii) allow the Product or data from the Product to be made available to any person other than Customer; (iii) assign, sell, transfer or pass along the data, the Product or access to the Product; (iv) translate, reverse engineer, decompile, disassemble or otherwise access the source code; and (v) provide services for a fee or otherwise use the Product without prior written agreement from Mitchell 1. Exhibit 2 at 75 (¶ 4(b)).

191. The 2016 Mitchell 1 EULA further provides that:

> Customer acknowledges and agrees that the Services and Product that is comprised of software, equipment and data, together with such other materials, data and information that Customer has access to or receives from Mitchell 1 (all such information and materials collectively called "Proprietary Materials") are the unique, valuable, confidential and proprietary product of Mitchell 1 and contain substantial trade secrets of Mitchell 1 and are entrusted to Customer in confidence to use only as expressly authorized in this Agreement. Customer shall,

> and shall cause its employees and any other third party, including its independent contractors, representatives, affiliates and agents, who, with the express consent of Mitchell 1, has access to such Proprietary Materials to keep all Proprietary Materials confidential and shall not disclose or permit access to the Proprietary Materials to any person or entity other than its employees for the purpose of attaining the objects of this Agreement; and to not use the Proprietary Materials for any purpose other than as expressly permitted herein. Exhibit 2 at 75 (¶ 9).

192. Autel US has breached the 2016 Mitchell 1 EULA by both exceeding the permitted purposes for access and use granted by the license and engaging in conduct prohibited by the license. Autel US has breached the 2020 Mitchell 1 Order Terms and Conditions at least by exceeding the permitted purposes for access and use granted by the license.

193. Autel US exceeded the 2016 Mitchell 1 EULA and 2020 Mitchell 1 Order Terms and Conditions' "permitted uses" and engaged in prohibited uses delineated in the 2016 Mitchell 1 EULA when it used Mitchell 1's ProDemand subscription services to steal large amounts of data from Plaintiffs' database servers instead of using the data for "(i) providing vehicle mechanical services; (ii) estimating vehicle mechanical parts and labor cost estimates; and (iii) conducting vehicle shop management." Exhibit 2 at 75 (¶ 4(a)); Exhibit 4 at 82 (¶ 4). Also, the 2016 Mitchell 1 EULA and the 2020 Mitchell 1 Order Terms and Conditions limit the purchased subscription (license) to the number of users on the order form. Autel US breached this provision by allowing multiple users from Autel ITC to access its ProDemand account.

194. Autel US also breached the 2016 Mitchell 1 EULA by using Mitchell 1's products ("the Product") in additional manners prohibited by the EULA. For example, upon information and belief, by providing Autel ITC access to ProDemand, Autel US "allow[ed] the Product or data from the product to be made available to any person other than Customer" and also "assign[ed], s[old],

transfer[red] or pass[ed] along the data, Product or access to the Product," which are prohibits uses. Exhibit 2 at 75 (¶ 4(b)).

195. As a result of Autel US's actions, Plaintiff Mitchell 1 has been harmed and has suffered damages in an amount to be proven at trial.

196. Further, Autel US's violations of these agreement have caused Plaintiffs Mitchell 1 irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Remedies at law are not adequate to fully compensate it for these injuries, entitling Mitchell 1 to injunctive relief.

SEVENTH CAUSE OF ACTION

Trespass to Chattels
(Against Both Defendants)

197. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 as if fully set forth herein.

198. Upon information and belief, Autel US and Autel ITC each committed a trespass to Plaintiffs' chattels under California law for interfering with Plaintiffs' data servers, data, products, and computer system.

199. Plaintiffs had, and have, a possessory interest in their data servers, proprietary diagnostic and repair data, and the computer system and products to which customers subscribe to gain access to that data and system.

200. Autel US and Autel ITC intentionally interfered with Plaintiffs' use or possession of their data servers, data, computer system, and products through their spoofing of Snap-on devices and extensive and repeated wrongful requests for data from the data servers. Autel US and Autel ITC bombarded Plaintiffs' network and data servers with hundreds of thousands or millions of requests over compressed time periods, at times spoofing dozens of devices from a single IP address to carry out their raid on Plaintiffs' data.

201. As described in more detail above, as a result of Autel US and Autel ITC each knowingly and without permission spoofing multiple handheld diagnostic

computers, and extensively attacking Plaintiffs' data servers, service to Plaintiffs' customers was cut off or interrupted, and Plaintiffs were forced to shut down worldwide access to customers on their data servers on multiple occasions.

202. Plaintiffs did not consent to Autel US or Autel ITC requesting this data.

203. In addition, Autel US and Autel ITC conspired with one another to commit trespass to chattels through the conduct described above. Autel US and Autel ITC conspired, agreed, and had a common plan and design, to work together to carry out mass attacks to siphon the proprietary data from the data servers associated with handheld diagnostic devices, and gained improper access to these data servers from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted activity, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful conduct described above.

204. Plaintiffs were harmed as a result of Autel's conduct. Defendants' extensive and repeated wrongful requests for information significantly slowed down Plaintiffs' network, customers were cut off from access to their account, and Plaintiffs were forced to shut down access to their databases for a segment of their customers on multiple occasions.

205. Plaintiffs are entitled to recover damages caused by Autel's conduct. In addition, Autel's trespass to chattels has caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts.

Remedies at law are not adequate to fully compensate Plaintiffs for these injuries, entitling Plaintiffs to injunctive relief.

EIGHTH CAUSE OF ACTION

Misappropriation of Trade Secrets under the DTSA (Against Both Defendants)

206. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 as if fully set forth herein.

207. Plaintiffs' compilation of proprietary diagnostic and repair information—including at least the specific categories of information known as Top Repairs, Top 10 Repairs, Real Fixes, Troubleshooting, Smart Data, Functional Tests, and Component Tests—are trade secrets within the meaning of the DTSA.

208. Plaintiffs invested substantial time and resources in developing the proprietary diagnostic and repair information described in this Complaint. As described in detail above, this information is derived from billions of real world repair records that were accumulated over a period of over 25 years, and that have been extensively reviewed and analyzed by Plaintiffs' experts and through artificial intelligence. Plaintiffs have invested substantial amounts of money, analysis, and product development to incorporate this proprietary data into their products and services in a highly useful form, over many years.

209. This comprehensive compilation of data derives significant economic value from not being known to others in the industry, and provides Plaintiffs with a substantial competitive advantage in the marketplace. No competitor has a comparable set of comprehensive data.

210. Plaintiffs have exercised reasonable efforts to maintain the confidentiality of this compilation of data. Among other things, the data is maintained on a password-protected network and on password-protected servers, which are accessible only to those with a need to use them. Plaintiffs limit access to the data internally at the company and employees who do have access to the data

are required to maintain it in confidence. Visitors to the Plaintiffs' facilities are required to sign in and to have an employee escort. In addition, the full compilation of data is never shared with others and when subsets are shared they are shared pursuant to confidentiality agreements.

211. The compilation of data is also not readily ascertainable by others or made publicly available. While individual users of Plaintiffs' products are allowed to have access to individual items of data, they are required to sign EULAs that require them to limit their use of the data. *See* Exhibit 6 at 87; Exhibit 2 at 75 (¶¶ 4(a)-(b)). The Mitchell 1 EULA further requires end users to acknowledge and agree to the confidentiality of the data. Exhibit 2 at 75 (¶ 9).

212. In addition, Plaintiffs' products are designed such that individuals do not gain access to the compilation as a whole. As described in more detail above, users of Plaintiffs' handheld diagnostic computers only gain access to proprietary diagnostic and repair information when the device is connected to a vehicle's OBD-II port and reading trouble codes. This means that a user must connect their device to a vehicle or have built a vehicle emulator for the device, which would need to be custom made. Moreover, even when a device is connected to a vehicle, the diagnostic information presented via the device's software is limited to data that corresponds to the make/model/vintage of the vehicle and the particular repair at issue. And the devices themselves are protected through the technological measures described above. Collectively, these technological measures meaningfully control access to Plaintiffs' proprietary compilation of data.

213. While certain aspects of this proprietary data (Top Repairs, Real Fixes, and Troubleshooting) are also available through ProDemand, again, only for the particular trouble codes at issue, access to that product is protected by the security measures described above, including a required user name and password, (or an approved IP address for certain customers only by agreement with Autel), usage is limited by the Mitchell 1 EULA, and Plaintiffs have an anti-piracy team that

monitors the accounts to ensure that customers are not exceeding their permitted usage.

214. In addition to the above, the maximum and minimum values of the "known good ranges" for the PID data is never shared with the end user, even at an individual level. For example, a user connecting a diagnostic device to a 2015 Toyota Camry with a particular issue code will only be able to view whether the PIDS associated with that data fall inside or outside the acceptable range. The range itself is never disclosed.

215. Determining the "known good ranges" for the PID data for all of the vehicles in Plaintiffs' databases was an enormous task that took years of analysis by experts, who were leveraging the billions of real world repair orders that are uniquely in the possession of Plaintiffs.

216. Autel US and Autel ITC improperly gained access to this trade secret information by circumventing the security measures that protected access to the devices and required authorization for individual data queries, then spoofing the devices to gain access to Plaintiffs' data servers, utilizing bots to scrape the data far faster than a human person could, making millions of requests from over 300 different IP addresses, and fully bypassing the required procedure of connecting the devices to a vehicle to obtain information that is pertinent only to the active problem codes for that vehicle for a particular repair. Autel US and Autel ITC were well aware that this was improper and egregious conduct. It was intended to acquire the compilation of data itself, or a substantial portion of it, rather than to access individual data points for the purpose of conducting repairs.

217. In addition, Autel US and Autel ITC conspired with one another to misappropriate Plaintiffs' trade secrets through the conduct described above. Autel US and Autel ITC conspired, agreed, and had a common plan and design, to work together to carry out mass attacks to misappropriate Plaintiffs' trade secrets from the data servers associated with handheld diagnostic devices, and gained improper

access to these data servers from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted activity, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful conduct described above.

218. The misappropriation of trade secrets by Autel US and Autel ITC was willful, malicious, and fraudulent—deliberately concealing the true source of the attack on Plaintiffs' data.

219. As a result of Autel's misappropriation, Plaintiffs have been damaged in an amount to be proven at trial. Further, Autel has been unjustly enriched by having the benefit of Plaintiffs' data that took many years to accumulate, review, and analyze.

220. As a result of Autel's trade secret misappropriation, Plaintiffs are entitled to recover damages both for the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation, or in the alternative to a reasonable royalty.

221. In addition, because Defendants' misappropriation of trade secrets was willful and malicious, Plaintiffs are entitled to exemplary damages in an amount up to two times the amount of the damages awarded, and to recover attorneys' fees and costs pursuant to 18 U.S.C. § 1836(b)(3).

222. Further, Autel's misappropriation of Plaintiffs' trade secrets has caused, and will continue to harm, irreparable harm to Plaintiffs, and Plaintiffs are entitled to injunctive relief.

NINTH CAUSE OF ACTION

Misappropriation of Trade Secrets under the California Uniform Trade Secrets Act
(Against both Defendants)

223. Plaintiffs restate and incorporate by reference Paragraphs 1 through 120 and 206 through 222 as if fully set forth herein.

224. Plaintiffs' compilation of proprietary diagnostic and repair information—including at least the specific categories of information known as Top Repairs, Top 10 Repairs, Real Fixes, Troubleshooting, Smart Data, Functional Tests, and Component Tests—are trade secrets within the meaning of the California Uniform Trade Secrets Act.

225. Plaintiffs invested substantial time and resources in developing the proprietary diagnostic and repair information described in this Complaint. As described in detail above, this information is derived from billions of real world repair records that were accumulated over a period of over 25 years, and that have been extensively reviewed and analyzed by plaintiffs' experts and through artificial intelligence. Plaintiffs have invested substantial amounts of money, analysis, and product development to incorporate this proprietary data into their products and services in a highly useful form, over many years.

226. This comprehensive compilation of data derives significant economic value from not being known to others in the industry, and provides Plaintiffs with a substantial competitive advantage in the marketplace. No competitor has a comparable set of comprehensive data.

227. Plaintiffs have exercised reasonable efforts to maintain the confidentiality of this compilation of data. Among other things, the data is maintained on a password-protected network and on password-protected servers, which are accessible only to those with a need to use them. Plaintiffs limit access to the data internally at the company and employees who do have access to the data are required to maintain it in confidence. Visitors to the Plaintiffs' facilities are

required to sign in and to have an employee escort. In addition, the full compilation of data is never shared with others and when subsets are shared they are shared pursuant to confidentiality agreements.

228. The compilation of data is also not readily ascertainable by others or made publicly available. While individual users of Plaintiffs' products are allowed to have access to individual items of data, they are required to sign EULAs that require them to limit their use of the data. *See* Exhibit 6 at 87; Exhibit 2 at 75 (¶¶ 4(a)-(b)). The Mitchell 1 EULA further requires end users to acknowledge and agree to the confidentiality of the data. Exhibit 2 at 75 (¶ 9).

229. In addition, Plaintiffs' products are designed such that individuals do not gain access to the compilation as a whole. As described in more detail above, users of Plaintiffs' handheld diagnostic computers only gain access to the proprietary diagnostic and repair information when the device is connected to a vehicle's OBD-II port and reading trouble codes. This means that a user must connect their device to a vehicle or have built a vehicle emulator for the device, which would need to be custom made. Moreover, even when a device is connected to a vehicle, the diagnostic information presented via the device's software is limited to data that corresponds to the make/model/vintage of the vehicle and the particular problems at issue. And the devices themselves are protected through the technological measures described above. Collectively, these technological measures meaningfully control access to Plaintiffs' proprietary compilation of data.

230. While certain aspects of this proprietary data (Top Repairs, Real Fixes, and Troubleshooting) are also available through ProDemand, again, only for the particular trouble codes at issue, access to that product is protected by the security measures described above, including a required user name and password, (or an approved IP address for certain customers only by agreement with Autel), usage is limited by the Mitchell 1 EULA, and Plaintiffs have an anti-piracy team that

monitors the accounts to ensure that customers are not exceeding their permitted usage.

231. In addition to the above, the maximum and minimum values of the "known good ranges" for the PID data is never shared with the end user, even at an individual level. For example, a user connecting a diagnostic device to a 2015 Toyota Camry with a particular issue code will only be able to view whether the PIDS associated with that data fall inside or outside the acceptable range. The range itself is never disclosed.

232. Determining the "known good ranges" for the PID data for all of the vehicles in Plaintiffs' databases was an enormous task that took years of analysis by experts, and it required the billions of real world repair orders that are uniquely in the possession of Plaintiffs.

233. Autel US and Autel ITC improperly gained access to this trade secret information by circumventing the security measures that protected access to the devices and required authorization for individual data queries, and then spoofing the devices to gain access to Plaintiffs' data servers, utilizing bots to scrape the data far faster than a human person could, making millions of requests from dozens of different IP addresses, and fully bypassing the required procedure of connecting the devices to a vehicle to obtain information that is pertinent only to the active problem codes for that vehicle for a particular repair. Autel US and Autel ITC were well aware that this was improper and egregious conduct. It was intended to acquire the compilation of data itself, or a substantial portion of it, rather than to access individual data points for the purpose of conducting repairs.

234. In addition, Autel US and Autel ITC conspired with one another to misappropriate Plaintiffs' trade secrets through the conduct described above. Autel US and Autel ITC conspired, agreed, and had a common plan and design, to work together to carry out mass attacks to misappropriate Plaintiffs' trade secrets from the data servers associated with handheld diagnostic devices, and gained improper

access to these data servers from IP addresses associated with Autel US as well as from Chinese IP addresses associated with Autel ITC. At least seven different "spoofed" ZEUS devices were observed attempting to improperly access Snap-on's data servers from both an Autel US IP address and various IP addresses from China associated with this scraping activity. As just one example of this concerted activity, on March 8, 2021, parallel requests for the same PID data from a 2015 Chevy Cruze were made from the main Autel US IP address and a Chinese IP address within one minute of each other. Autel US and Autel ITC carried out the conspiracy by engaging in the wrongful conduct described above.

235. The misappropriation of trade secrets by Autel US and Autel ITC was willful, malicious, and fraudulent—deliberately concealing the true source of the attack on Plaintiffs' data.

236. As a result of Autel's misappropriation, Plaintiffs have been damaged in an amount to be proven at trial. Further, Autel has been unjustly enriched by having the benefit of Plaintiffs' data that took many years to accumulate, review, and analyze.

237. As a result of Autel's trade secret misappropriation, Plaintiffs are entitled to recover damages both for the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation, or in the alternative to a reasonable royalty.

238. In addition, because Defendants' misappropriation of trade secrets was willful and malicious, Plaintiffs are entitled to exemplary damages in an amount up to two times the amount of the damages awarded, and to recover attorneys' fees and costs pursuant to California Civil Code sections 3426.3 and 3426.4.

239. Further, Autel's misappropriation of Plaintiffs' trade secrets has caused, and will continue to harm, irreparable harm to Plaintiffs, and Plaintiffs are entitled to injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

a. For temporary, preliminary, and permanent injunctive relief, including but not limited to requiring Defendants to cease taking information from Plaintiffs, and prohibiting Defendants from making use of any information obtained from Plaintiffs or any features that incorporate information from Plaintiffs;

b. For damages sufficient to fully compensate Plaintiffs for all of the harm caused by Defendants' actions and for having to respond to Defendants' actions;

c. For profits of Defendants pursuant to 17 U.S.C. § 1203(c)(2) or otherwise allowable by law;

d. For statutory damages pursuant to 17 U.S.C. § 1203(c)(3) or otherwise allowable by law;

e. For damages sufficient to compensate for the unjust enrichment of Defendants gained through their misappropriation of Plaintiffs' trade secrets;

f. Alternatively, in lieu of damages for actual loss or for unjust enrichment from Defendants' misappropriation of Plaintiffs' trade secrets, for a reasonable royalty;

g. For exemplary damages up to two times the amount of damages awarded for Defendants' misappropriation of Plaintiffs' trade secrets pursuant to 18 U.S.C. § 1836(b)(3) and Cal. Civ. Code § 3426.3;

h. For exemplary and/or punitive damages as otherwise allowable by law;

i. For attorneys' fees pursuant to 17 U.S.C. § 1203(b), 18 U.S.C. § 1836(b)(3), Cal. Civ. Code § 3426.4, and section 20 of the Mitchell 1 EULA, or as otherwise allowable by law;

j. For costs of this action;

k. For pre-and post-judgment interest;

l. For such other and further relief as the Court may deem just and proper.

Plaintiffs demand a jury trial on all claims that are triable by jury.

Dated: July 27, 2021

MORRISON & FOERSTER LLP

By: */s/ Kenneth A. Kuwayti*

KENNETH A. KUWAYTI
KKuwayti@mofo.com

Attorneys for Plaintiffs
MITCHELL REPAIR
INFORMATION COMPANY, LLC
and SNAP-ON INCORPORATED