



IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

THE STATE OF DELAWARE, ex rel.	:	
Kathleen Jennings, Attorney General	:	
of the State of Delaware,	:	
	:	
Plaintiff	:	C.A. No.
v.	:	
	:	
GENERAL MOTORS LLC,	:	
a limited liability company;	:	
GENERAL MOTORS HOLDINGS LLC,	:	
a limited liability company;	:	
and ONSTAR, LLC,	:	
a limited liability company,	:	
	:	
Defendants.	:	

CONSENT JUDGMENT

Plaintiff the State of Delaware, *ex rel.*, Kathleen Jennings, Attorney General for the State of Delaware(the “State” or the “Plaintiff”), and Defendants General Motors LLC, General Motors Holdings LLC, and OnStar, LLC (collectively “GM” or “Defendants”) (Defendants together with the State, the “Parties”), have agreed to the stipulations and terms of this Consent Judgment (“Judgment”) without admission of any facts or liability as alleged in the Complaint, and with all Parties having waived their right to appeal.¹

¹ Defendants are simultaneously entering into similar judgments with the Attorneys General or appropriate representatives of the states of Alabama, Alaska, Arizona, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota,

This Judgment resolves the Plaintiff's investigation of Defendants' data collection and sharing practices described in the Complaint regarding Defendants' compliance with the Consumer Fraud Act, 6 *Del. C.* §§ 2511, *et seq.*, and the Uniform Deceptive Trade Practices Act, 6 *Del. C.* §§ 2531, *et seq.* The Parties stipulate that the Court may enter this Judgment.

I. PARTIES AND JURISDICTION

1. Plaintiff in this case is the State of Delaware, *ex rel.*, Kathleen Jennings, Attorney General for the State of Delaware. The Attorney General is charged with enforcement of the Consumer Fraud Act and the Uniform Deceptive Trade Practices Act pursuant to 6 *Del. C.* §§ 2522, 2533 and 29 *Del. C.* § 2522.

2. Defendant General Motors LLC is a Delaware limited liability company with its principal office or place of business at 300 Renaissance Center, Suite L1, Detroit, Michigan 48243. General Motors LLC is a wholly owned subsidiary of General Motors Company, a Delaware corporation.

3. Defendant General Motors Holdings LLC is a Delaware limited liability company with its principal office or place of business at 300 Renaissance Center, Suite L1, Detroit, Michigan 48243. General Motors Holdings LLC is a wholly owned subsidiary of General Motors Company, a Delaware corporation.

Utah, Vermont, Virginia, Washington, Wisconsin, and the District of Columbia (collectively, "Attorneys General").

4. Defendant OnStar, LLC is a Delaware limited liability company with its principal office or place of business at 400 Renaissance Center, Detroit, Michigan 48243. OnStar, LLC is a wholly owned subsidiary of General Motors Company, a Delaware corporation.

5. At all relevant times, Defendants were engaged in trade and commerce affecting consumers in Delaware insofar as Defendants manufactured, advertised, and distributed Vehicles in Delaware, including Vehicles under the Chevrolet, GMC, Cadillac, and Buick brands to General Motors-authorized dealerships that were then sold to consumers. Defendants were also in possession of the Covered Driver Data of Delaware residents.

6. The Court has jurisdiction over the subject matter of this action and jurisdiction over the Parties for purpose of entering and enforcing this Judgment and venue is proper in this Court pursuant to 10 *Del. C.* §§ 341 *et seq.* and 6 *Del. C.* §§ 2523, 2533.

II. DEFINITIONS

For the purposes of this Judgment, the following definitions shall apply:

7. “Affiliate” means a U.S. entity that is controlled, directly or indirectly, by the Defendants.

8. “Affirmative Express Consent” means a clear affirmative act signifying a Consumer’s freely given, specific, informed and unambiguous agreement to allow

the processing of Covered Driver Data relating to the Consumer, following a Clear and Conspicuous disclosure to the individual. For purposes of obtaining Affirmative Express Consent, a clear affirmative action means a Consumer's consent is communicated through either (a) deliberate and clear conduct, or (b) a statement that clearly indicates their acceptance of the proposed processing of their Covered Driver Data.

The following do not constitute Affirmative Express Consent:

- a. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the Consumer;
- b. Acceptance of general or broad terms of use or a similar document that contains descriptions of Covered Driver Data processing along with other, unrelated information;
- c. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice; or
- d. Silence, inactivity or inaction, pre-ticked boxes, and other negative option opt-out constructions that require intervention from the Consumer to prevent agreement.

9. "Clear(ly) and Conspicuous(ly)" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by Consumers, including in all of the following ways:

- a. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made through only one means;
- b. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood;
- c. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for Consumers to easily hear and understand it;
- d. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable and if the interactive electronic medium is a component of a Vehicle such as an infotainment head unit, it should be displayed at a time and in a manner that would not interfere with Vehicle operation;
- e. The disclosure must use plain, straightforward language, diction and

syntax, and avoid technical or legal jargon;

- f. The disclosure must be reasonably accessible to Consumers with disabilities including through the use of digital accessibility tools;
- g. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications;
- h. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication; and
- i. The disclosure must be made through a readily accessible interface regularly used in conjunction with the Defendants' products or services.

10. "Consumer" means a natural person in Delaware.

11. "Consumer Privacy Law" means the Delaware citation(s) set forth in Exhibit A.

12. "Consumer Protection Law" means the Delaware citation(s) set forth on Exhibit A.

13. "Consumer Reporting Agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to other parties and which uses any means or facility of interstate commerce for the purpose

of preparing or furnishing consumer reports.

14. a. “Covered Driver Data” means information collected by Defendants that:

- i. Originates from a Vehicle or a General Motors-branded mobile application (“App”), or derived data (such as data generated algorithmically) from information originating from a Vehicle or App; and
- ii. Is Location Data or is one of the following events linked or Reasonably Linkable to a Consumer:
 - a) radio listening data regarding specific content, channel, or station; or
 - b) driver behavior information regarding hard braking, hard acceleration, hard cornering, crossing of a designated high-speed threshold, seat belt usage, or late-night driving; and trip time and duration for such events.
- b. Covered Driver Data excludes data (i) related to build, trim, make, model, and year of the Vehicle or (ii) that is Deidentified post-collection.
- c. For purposes of this definition, “Reasonably Linkable” means any use of a unique persistent identifier, such as a Vehicle Identification

Number (“VIN”) or an alternative identifier that can be linked back to a VIN, when the unique persistent identifier or alternative identifier is combined or associated with Covered Driver Data.

15. “Deidentified” or “Deidentifiable” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, in that Defendants must, at a minimum:

- a. Have implemented technical safeguards to prohibit reidentification of the person to whom the information may pertain;
- b. Have implemented business processes that specifically prohibit reidentification of the information, including by buyers, customers, or other entities to whom Defendants provide the information;
- c. Have implemented business processes to prevent inadvertent release of Deidentified information; and
- d. Make no attempt to reidentify the information.

Data that is linked to a unique identifier, such as a VIN, or an alternative identifier that can be linked back to a VIN, or to a Vehicle’s garage address, is not Deidentified.

16. “Delete,” “Deleted,” or “Deletion” means to remove information such that it is not maintained in retrievable form and cannot be retrieved in the normal

course of business.

17. “Governance Process” means any written policy, standard, procedure, or process (or any combination thereof) designed to achieve a control objective.

18. “Effective Date” means November 30, 2026.

19. “High-Risk Processing Activity” means: (1) the sale of Covered Driver Data to the extent permitted by state law; and (2) the disclosure of Location Data to Third Parties.

20. “Insurance Affiliate(s)” means an Affiliate that is in the business of and authorized to transact personal lines of property/casualty insurance for Vehicles.

21. “Location Data” means any data collected by Defendants that reveals the precise location of a Vehicle, mobile device (in the case such information is obtained from an App), or Consumer, including but not limited to Global Positioning System (“GPS”) coordinates, fine location data, cell tower information, or precise location information inferred from basic service set identifiers (“BSSIDs”), WiFi Service Set Identifiers (“SSID”) information, or Bluetooth receiver information, or any unique persistent identifier combined with such data, such as a Vehicle’s VIN, or an alternative identifier that can be linked to a Vehicle’s VIN. Data that (1) reveals only a Vehicle’s, mobile device’s, or a Consumer’s coarse location (e.g., ZIP code or census block location with a radius of at least 1,850 feet), or (2) that is used solely for the purpose of generating such coarse location and then Deleted within 48 hours

of collection is not “Location Data.”

22. “OnStar” means the connected vehicle services branded as OnStar, or any other successor service that Defendants implement after the Effective Date that has the same or substantially the same functionality with regard to the collection of Covered Driver Data.

23. “Personal Information” means information that is linked or reasonably linkable to an individual Consumer.

24. “Service Provider” means any entity that (1) processes, uses, or receives data collected by or on behalf of Defendants for and at the direction of Defendants and no other individual or entity, (2) does not disclose data, or any individually identifiable information derived from such data, to an individual or entity other than Defendants or a subcontractor to such Service Provider bound to data processing terms no less restrictive than terms to which the Service Provider is bound, and (3) does not use data for any purpose other than performing the services specified in the Service Provider’s contract with Defendants.

25. “Third Party(ies)” means any individual or entity other than Defendants, Affiliates, or Service Providers.

26. “User” means a Consumer who has an OnStar account with a Vehicle garage address in Delaware.

27. “Vehicle” means a U.S. retail and General Motors-branded motor

vehicle, including Chevrolet, GMC, Cadillac, and Buick brands, that is owned by, sold or leased to, or used by an individual Consumer for their own personal use. Vehicle includes the components and embedded systems that were present when originally sold by Defendants, excluding Consumer-installed components. Vehicle does not include: motor vehicles that are owned by Defendants, Defendants' Affiliates or General Motors-branded dealers; motor vehicles that are sold or leased to, or used by, fleet or daily rental companies, suppliers, business organizations, or government entities; or scrapped or stolen vehicles.

III. INJUNCTIVE RELIEF

28. The duties, responsibilities, burdens, and obligations undertaken in connection with this Judgment shall apply to Defendants individually, collectively, or in any combination, and their successors.

29. The injunctive terms contained in this Judgment are entered into pursuant to the Consumer Fraud Act, 6 *Del. C.* § 2523, and the Uniform Deceptive Trade Practices Act, 6 *Del. C.* § 2533.

A. COMPLIANCE WITH LAW

30. Defendants must comply with the Consumer Protection Law and Consumer Privacy Law in connection with their collection, maintenance, use, disclosure, and safeguarding of Covered Driver Data and the Personal Information of Consumers collected to deliver OnStar services.

31. Defendants must not make any representations or omissions of fact capable of misleading Consumers regarding (a) the extent to which Defendants collect, maintain, use, or disclose any Covered Driver Data or Personal Information, or (b) the purposes for which Defendants collect, maintain, use, or disclose any Covered Driver Data or Personal Information, including uses Defendants authorized by any entity to whom the Defendants disclose Covered Driver Data or Personal Information.

B. PRIVACY PROGRAM

32. Privacy Program: Within one-hundred eighty (180) days of the Effective Date, Defendants must develop, implement, and maintain a comprehensive information privacy program governing (i) the collection, storage, and use of Covered Driver Data and the Personal Information of Consumers collected to deliver OnStar services, (ii) the disclosure of Covered Driver Data to Third Parties, and (iii) the disclosure of Personal Information to Third Parties when such data is combined with Covered Driver Data (“Privacy Program”). Defendants must document in writing the content and process to implement and maintain the Privacy Program. Any material changes to the Privacy Program must be documented. The Privacy Program must, at a minimum, include the specific privacy safeguards set forth in Paragraphs 32 through 57 of this Judgment. The Privacy Program obligations set forth in this Paragraph shall continue until January 13, 2046, provided, however, that

the following Paragraphs shall expire at a period of ten (10) years from the Effective Date: 36, 39, 47, and 52 through 55.

33. Chief Privacy Officer: Defendants must employ an individual who shall be responsible for oversight of the Privacy Program and Governance Processes relating to compliance with privacy laws, including the privacy requirements of the Consumer Protection Law and Consumer Privacy Law (hereinafter referred to as the “Chief Privacy Officer”). The Chief Privacy Officer must:

- a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role, and possess a fundamental understanding of state and federal privacy laws;
- b. Assist Defendants in complying with the privacy requirements of the Consumer Protection Law and Consumer Privacy Law;
- c. Have a process to coordinate with Defendants’ executives and officers as it relates to business operations affecting the privacy of Personal Information of Users and Covered Driver Data that Defendants collect, process, store, maintain, or transmit to Service Providers or Third Parties;
- d. At least once annually, provide to the Board of Directors, or through a committee of the Board that assists in providing oversight of Defendants’ privacy risks, a report on the privacy safeguards which

address internal and external risks to the privacy of Covered Driver Data and Personal Information of Users that Defendants collect, process, store, maintain, or disclose to Third Parties; and

e. Provide a report on the privacy safeguards as appropriate, but no less than quarterly to the General Counsel and annually to the Chief Executive Officer. Such report shall address internal and external risks to the privacy of Covered Driver Data and Personal Information of Users that Defendants collect, process, store, maintain, or disclose to Third Parties.

34. Necessary Resources and Support: Defendants must provide the Chief Privacy Officer, Privacy Program, and corresponding staff with the resources and support reasonably necessary so that the Privacy Program functions as required by this Judgment.

35. Existing Program or Safeguards: Defendants may satisfy the requirements to implement and maintain the Privacy Program required by this Judgment through review, maintenance, and, as necessary, updating, of an existing privacy program provided that such existing privacy program meets the requirements set forth in this Judgment.

36. Data Protection Assessment: Defendants must perform data protection assessments (“Data Protection Assessment”) in accordance with this paragraph. Data

Protection Assessments must:

- a. Be conducted prior to Defendants engaging in a new High-Risk Processing Activity;
- b. Identify and weigh the benefits that may flow, directly and indirectly, from the new High-Risk Processing Activity to Defendants and Users against the potential risks to the rights of the User associated with such processing, as mitigated by safeguards that can be employed by Defendants and, where relevant, their Service Providers to reduce such risks. Defendants must factor into any such Data Protection Assessment the reasonable expectations of Users, as well as the context of the processing and the relationship between Defendants and the User whose Covered Driver Data will be processed;
- c. For new High-Risk Processing Activities, consider and address:
 - i. The business purpose for the High-Risk Processing Activity; and
 - ii. Whether the High-Risk Processing Activity is reasonably necessary for the stated business purpose.

C. PRIVACY PROGRAM: SPECIFIC SAFEGUARDS

37. Data Minimization: Defendants must limit collection of Covered Driver Data to what is adequate, relevant, and reasonably necessary to fulfill the specific

purpose for which it was collected, as disclosed to the Consumer.

38. Purpose Limitations: Defendants must, use, disclose, or retain Covered Driver Data only for purposes that are reasonably necessary for the purpose for which such Covered Driver Data was collected, or as otherwise consistent with Paragraph 42.b.

39. Covered Driver Data Inventory – OnStar: Defendants must develop and maintain an inventory of any category of Covered Driver Data that OnStar collects and Defendants disclose to a Third Party or to an Insurance Affiliate.

40. Privacy Notice: Defendants must provide Consumers with a privacy notice (“Privacy Notice”) that utilizes consistent terminology regarding Covered Driver Data throughout the Privacy Notice and Clearly and Conspicuously discloses:

- a. the categories of Covered Driver Data that Defendants collect;
- b. the source of the Covered Driver Data that will be collected;
- c. the specific purpose(s) for which Covered Driver Data is collected, used, or disclosed;
- d. any permissible secondary purpose(s) that Defendants anticipate at the time of collection for which Defendants will use Covered Driver Data, including whether such Covered Driver Data is used for usage-based insurance or targeted advertising, if allowed by state law;
- e. how long Covered Driver Data will be retained by Defendants;

- f. the categories of Third Parties, including, where applicable, Consumer Reporting Agencies to whom Defendants disclose Covered Driver Data; and
- g. how Consumers may exercise their consumer rights regarding their Covered Driver Data (“Privacy Notice”).

41. Privacy Notice Changes: Defendants must Clearly and Conspicuously communicate to Consumers material changes to the Privacy Notice regarding Covered Driver Data as soon as reasonably practical before the change is implemented. In addition to posting a new effective date at the top of the Privacy Notice, Defendants must either e-mail notices to Users who have valid e-mail addresses on file with Defendants or otherwise make reasonable efforts to notify Consumers summarizing the material changes. To the extent that any material change to the Privacy Notice includes processing Covered Driver Data for any new purposes or new secondary purposes that are not covered under the Affirmative Express Consent exceptions in Paragraph 42.b, Defendants must obtain the Consumer’s Affirmative Express Consent in accordance with Paragraph 42 before processing.

42. Limitations on Collection, Use, and Disclosure of Covered Driver Data Without Affirmative Express Consent: Defendants must obtain the relevant Consumer’s Affirmative Express Consent prior to collecting or using such

Consumer's Covered Driver Data, or disclosing such Consumer's Covered Driver Data to any Third Party.

a. Each separate, unrelated service or feature that collects, uses, or discloses Covered Driver Data requires Defendants to obtain a separate Affirmative Express Consent. For the avoidance of doubt, this includes services or features provided by Insurance Affiliates that collect, use, or disclose Covered Driver Data.

b. Notwithstanding the above, Affirmative Express Consent is not required when Defendants collect, use, or disclose Covered Driver Data for the following purposes:

- i. To disclose Covered Driver Data to emergency responders;
- ii. To respond to a consumer-initiated communication originating from within the Vehicle or App, where Covered Driver Data may be collected, used, or disclosed only to provide that response;
- iii. To respond to a Vehicle-initiated communication related to the safe operation of that Vehicle where Covered Driver Data may be collected, used, or disclosed only to provide that response;
- iv. To comply with lawful governmental requests, regulatory requirements, and legal orders, or for use to prepare for or defend against product liability, breach of contract, consumer protection, or warranty claims;
- v. To conduct research or efforts to improve, repair, or enhance

safety of, or develop products, services, or technology, provided, however that (1) only Deidentified Covered Driver Data is disclosed to Third Parties to fulfill this purpose; and (2) marketing is excluded from this purpose;

vi. To conduct investigations of potential product quality or safety issues; to determine or effectuate Vehicle field actions, including customer satisfaction campaigns, technical service bulletins, compliance recalls, and safety recalls; to detect or respond to cybersecurity incidents; or to administer and fulfill Vehicle warranties; and

vii. To perform diagnostics and prognostics of components of the Vehicle; or to identify and address issues that impair existing functionality, provided, however, that only Deidentified Data is disclosed to Third Parties to fulfill this purpose unless identification is necessary to address diagnostic or prognostic issues relating to specific Vehicles.

c. For avoidance of doubt, Defendants may collect data for Affiliates' use consistent with Paragraphs 42 and 43.

43. Affirmative Express Consent Process: Whenever Affirmative Express Consent is requested from a Consumer pursuant to this Judgment, Defendants must provide the Consumer with a Clear and Conspicuous disclosure prior to requesting such consent.

a. The disclosure (s) required by this Paragraph must state (1) the

categories of information that will be collected; (2) each specific purpose(s) for which the information is being collected, used, or disclosed; (3) the names or categories of any Third Parties to whom the information is disclosed, provided, however, that if Defendants seek consent by specifying categories of Third Parties, Defendants must also provide a hyperlink to a separate, regularly updated web page listing the names of those Third Parties; and (4) a simple, easily located means by which the Consumer can withdraw consent and that describes any limitations on the Consumer's ability to withdraw consent.

- b. Each Clear and Conspicuous disclosure required by this Paragraph must be separate from any "privacy policy," "terms of service," "terms of use," or other similar consumer-facing disclosure.
- c. If Defendants disclose Covered Driver Data to a Third Party for usage-based insurance purposes, they must obtain Affirmative Express Consent consistent with Paragraph 43.a and b and disclose to Users that such data may be used for usage-based insurance rates or coverage.

44. Consumer Notice Regarding OnStar Enrollment: Within one-hundred eighty (180) days of the Effective Date, Defendants must provide Users that enrolled in OnStar prior to the Effective Date with a notice directing them to the current OnStar Affirmative Express Consent disclosure as described in Paragraph 43 of this

Judgment, which disclosure will include information about how to withdraw Affirmative Express Consent and unenroll from OnStar.

45. Withholding or Withdrawal of Affirmative Express Consent:

Defendants must allow and must not limit a Consumer's ability to withhold or withdraw Affirmative Express Consent for the collection, use, or disclosure to Third Parties of Covered Driver Data, such as by degrading the quality of functionality of a product or service as a penalty for withholding or withdrawing such Affirmative Express Consent, unless the collection and use of Covered Driver Data is technically necessary to provide the quality or functionality of the product or service without such degradation.

46. Disabling Location Setting: Defendants must allow Consumers to disable the collection of Location Data from their Vehicles, to the extent the Vehicle is equipped with the necessary technology, which may be accomplished by providing a mechanism such as a toggle on the Vehicle for Consumers to disable the collection of Location Data, provided, however, that even if the collection of Location Data is disabled on the Vehicle, Defendants may:

a. Respond to a Consumer-initiated communication originating from within the Vehicle, or an App, where Location Data may be collected, used, or disclosed only to provide that response;

b. Respond to a Vehicle-initiated communication related to either the safe

operation of that Vehicle or a theft-related alert, where Location Data may be collected, used, or disclosed only to provide that response; and

c. Comply with lawful governmental requests, regulatory requirements, and legal orders, where Location Data may be collected, used, or disclosed as necessary for legal compliance.

47. Disclosure of Option to Disable Location: A Consumer's ability to disable the collection of Location Data in accordance with Paragraph 46 and where a Consumer can find instructions on how to do so must be communicated to the Consumer through a Clear and Conspicuous disclosure at or prior to the time the Affirmative Express Consent is requested in accordance with Paragraph 43, as well as in the Privacy Notice.

48. Declining Enrollment in OnStar: Defendants must allow Consumers to disable Defendants' remote collection of all data from their Vehicles if Consumers decline to enroll or choose to unenroll in OnStar.

a. Defendants must disclose to Consumers that they can disable Defendants' remote collection of all data from their Vehicle and the process for doing so. This must be disclosed to Consumers in the Privacy Notice and as part of any OnStar enrollment or cancellation process(es).

b. If the Consumer declines to enroll or unenrolls in OnStar, Defendants may:

i. Respond to a Consumer-initiated communication originating

from within the Vehicle, where data may be collected, used, or disclosed only to provide that response;

ii. Respond to a Vehicle-initiated communication related to the safe operation of that Vehicle, where data may be collected, used, or disclosed only to provide that response; and

iii. Collect, use, or disclose data to identify and address issues that impair safety or to provide over-the-air updates, and for no other purposes, provided, however, that prior to any collection, use, or disclosure of data for this purpose, Defendants must provide notice to Consumers regarding this collection, use, or disclosure, and provided, further, however, if Covered Driver Data is disclosed for this purpose, Defendants can only disclose Deidentified Covered Driver Data to Third Parties unless identification is necessary to address a safety issue for or provide over-the-air updates to a specific Vehicle.

49. Enrollment in OnStar: Within sixty (60) days of the Effective Date, Defendants must implement and maintain a policy and procedure for Consumers to enroll in OnStar by independent Consumer action, such as via email (“Enrollment Notice”). Such policy and procedure must include that any Consumer who does not act within ten (10) days of the Enrollment Notice will be treated as declining enrollment in OnStar as set out in Paragraph 48 of this Judgment. Prior to enrollment, Defendants may only collect Covered Driver Data for the purposes listed in

Paragraph 42.b. Defendants must implement a periodic review program to assess U.S. GM-authorized dealerships' compliance with the policy and procedure implemented pursuant to this Paragraph by sampling OnStar enrollments to identify anomalous enrollment patterns that may indicate noncompliance by such dealerships.

50. Employee Training – General: Defendants must provide employee training concerning its Privacy Program to employees who are responsible for implementing, maintaining, or evaluating the Privacy Program, including, but not limited to, the Chief Privacy Officer, and employees responsible for handling User inquiries about the Defendants' privacy practices on an ongoing and regular basis, no less than annually. In particular, such training must include privacy issues related to Consumer notice and Affirmative Express Consent. Defendants must document the trainings, including the date(s) upon which they were provided and to whom.

51. Employee Training – Special: In addition to the training required by Paragraph 50, employees who are responsible for implementing, maintaining, or evaluating the Privacy Program, including, but not limited to, the Chief Privacy Officer, must receive specialized training to help effectuate Defendants' compliance with the terms of this Judgment. Defendants must provide the training required under this Paragraph to all such employees within forty-five (45) days of the Effective Date of this Judgment or prior to any such employee starting their responsibilities for

implementing, maintaining, or evaluating the Privacy Program. Defendants must document the trainings, including the date(s) upon which they were provided and to whom.

D. PRIVACY PROGRAM: SERVICE PROVIDERS AND THIRD PARTIES

52. Due Diligence: Defendants must develop, implement, and maintain a Governance Process for selecting Service Providers and Third Parties capable of reasonably safeguarding the privacy of Covered Driver Data are consistent with Defendants' obligations under this Judgment. Defendants must follow such Governance Process prior to any new disclosure of Covered Driver Data to a Third Party or Service Provider or new permission for collecting Covered Driver Data by a Third Party or Service Provider that commences on or after the Effective Date.

53. Written Contracts: This Paragraph only applies to new written contracts or agreements between a Defendant and Service Provider or Third Party executed on or after the Effective Date.

a. Prior to disclosing Covered Driver Data to a Service Provider or Third Party, Defendants shall enter into a written contract or agreement with such Service Provider or Third Party requiring the Service Provider or Third Party to:

i. refrain from retaining, using, or disclosing the Covered Driver Data received from Defendants for any purposes other than those

specified in the contract or agreement or as otherwise permitted by law;

- ii. appropriately safeguard the confidentiality, integrity, and security of Covered Driver Data;
- iii. where applicable, Delete or securely return Covered Driver Data at the end of the provision of the services for which the Covered Driver Data was collected, unless retention is required to fulfill litigation holds, or to comply with lawful governmental requests, regulatory requirements, legal orders, or a documented accounting or tax obligation.

b. Defendants must develop, implement, and maintain a Governance Process to retain copies of such written agreements or contracts applicable to such Service Providers and Third Parties and any other documentation demonstrating a Service Provider's or Third Party's commitment to comply with the foregoing practices.

c. The contracting requirement set forth in this paragraph shall not apply to disclosures of Covered Driver Data that fall under Paragraph 42.b.

54. Governance: Defendants must develop, implement, and maintain a Governance Process to reasonably identify material inconsistencies between a Service Provider's and Third Party's use or disclosure of Covered Driver Data

received from Defendants and the terms of any written contract or agreement such Service Provider or Third Party has with Defendants that is required under Paragraph 53.a and b, Defendants shall retain documentation of such efforts. The Governance Process may include self-certifications, audits, assessments, reviews, testing, or other reasonable means of examining of Service Providers' or Third Parties' use of Covered Driver Data received from Defendants. The frequency, type, number, variety, and/or robustness of such examination shall be based on documented factors such as the nature of the products, programs, and services provided by the Service Provider or Third Party, and the type and volume of Covered Driver Data provided to the Service Provider or Third Party.

- a. Where any Service Provider or Third Party is required to provide self-assessment questionnaires to Defendants, Defendants must seek corroboration as appropriate based upon the circumstances which may include supporting documentation as well as follow-up with those Service Providers and Third Parties.

55. Materially Inconsistent Practices: Defendants must develop, implement, and maintain a Governance Process to take reasonable and appropriate action concerning any Service Provider or Third Party that Defendants know is using Covered Driver Data in a manner materially inconsistent with the terms of any written agreement or contract such Service Provider or Third Party has with

Defendants that is required under Paragraph 53.

56. Deletion of Previously Disclosed Covered Driver Data: Defendants must:

a. Request Third Parties with whom Defendants disclosed Covered Driver Data prior to January 16, 2025 to Delete such data, except when subject to legal or regulatory requirements (including litigation holds); and

b. Not sell or disclose Covered Driver Data to any Third Party with whom Defendants previously disclosed Covered Driver Data until (1) that Third Party confirms receipt of the request required by subparagraph a, except when subject to legal or regulatory requirements (including litigation holds) as set out in Paragraph 42.b and (2) to the extent the Third Party is a Consumer Reporting Agency, the Consumer Reporting Agency provides Defendants written confirmation that the Covered Driver Data has been Deleted or that such Covered Driver Data is subject to legal or regulatory requirements that prevent Deletion.

E. PRIVACY PROGRAM: GENERAL MOTORS-AUTHORIZED DEALERSHIPS

57. Dealer-Related Obligations: Within sixty (60) days of the Effective Date, Defendants must develop and implement dealer training and program materials that instruct General Motors-authorized dealership personnel that Consumers be given the opportunity to review applicable privacy disclosures and must accept those disclosures themselves prior to enrollment in OnStar.

F. PRIVACY PROGRAM: THIRD-PARTY ASSESSMENTS

58. Privacy Program Assessment: Within ninety (90) days of the Effective Date, Defendants must engage an independent third party (“Third-Party Assessor”) to conduct an assessment of the Privacy Program required by this Judgment (Paragraphs 32 through 57) (“Third-Party Privacy Assessment”). The Third-Party Assessor must have the background and experience necessary to evaluate the effectiveness of Defendants’ Privacy Program. The Third-Party Assessment must:

- a. Determine whether Defendants have implemented and maintained the Privacy Program required by Paragraphs 32 through 36 regarding Covered Driver Data and the disclosure of Personal Information to Third Parties when such data is combined with Covered Driver Data;
- b. Assess the effectiveness of Defendants’ implementation and maintenance of the specific privacy controls required in Paragraphs 37 through 57;
- c. Identify any gaps or weaknesses in, or instances of material non-compliance with the privacy controls assessed in subparagraph b; and
- d. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Third-Party

Assessor examined is (a) appropriate for assessing an enterprise of the Defendants' size, complexity, and risk profile; and (b) sufficient to justify the Third-Party Assessor's findings.

59. The reporting period for the Third-Party Assessments must cover: (1) the first three hundred and sixty-five (365) days after the Effective Date for the initial Third-Party Assessment (the "Initial Assessment Date"); and (2) each two-year period thereafter for four (4) years after the Initial Assessment Date for the biennial Third-Party Assessments.

60. The Third-Party Assessor must prepare a report including its findings and recommendations ("Third-Party Assessment Report"). The Defendants must provide a copy of the Third-Party Assessment to the Washington State Attorney General within thirty (30) days of receipt from the Third-Party Assessor.

61. The Washington State Attorney General may provide a copy of any Third-Party Assessment Report received from Defendants to Plaintiff upon request.

G. CONSUMER-RELATED RELIEF

62. Deletion Option: Defendants must provide an easily-located method by which a Consumer may request Deletion of the Consumer's Covered Driver Data. The method chosen must: (1) consider the ways in which Consumers normally interact with Defendants; (2) enable the Consumer to submit the request to the Defendants at any time; (3) be described through a Clear and Conspicuous

disclosure; and (4) be easy for Consumers to execute, requiring a minimal number of steps. Upon request by a Consumer to exercise the Deletion option, Defendants must provide confirmation of receipt of the Consumer's request. Defendants may require a Consumer to provide Defendants with information necessary to complete such request but must not use, provide access to, or disclose any information collected for the request for any other purpose. The obligations set forth in this Paragraph shall continue until January 13, 2046.

- a. If Defendants identify that the Consumer resides in a U.S. jurisdiction that provides the Consumer with Deletion rights, Defendants must process the Consumer's request in compliance with the law of that jurisdiction.
- b. If Defendants identify that the Consumer does not reside in a U.S. jurisdiction that provides the Consumer with Deletion rights, Defendants must process the Consumer's deletion request in accordance with this subparagraph. Once Defendants verify that the Consumer is a Consumer for whom Defendants possess Covered Driver Data, within sixty (60) days, Defendants must process the Consumer's deletion request and notify the Consumer that the request has been processed.
- c. Nothing in subparagraph b shall abrogate Defendants' rights to: (i) avail

themselves of any and all rights, exceptions, and exemptions existing under any state or federal law or (ii) retain a subset of a Consumer's Covered Driver Data to comply with their legal, regulatory, or other obligations. Defendants are not obligated to comply with the requirements under subparagraph b when the requirements conflict with Defendants' ability to comply with federal, state, or local laws or regulations; any civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; or any transactional, tax, escheatment, corporate accountability, or other legitimate business need compatible with the context in which the Consumer provided the information.

63. Deletion of Prior-Retained Covered Driver Data: Within one hundred and eighty (180) days of the Effective Date, Defendants must:

- a. Delete or destroy all Covered Driver Data retained prior to January 16, 2025, except when Covered Driver Data is retained for and necessary to fulfill the following purposes: (a) litigation holds; (b) to comply with lawful governmental requests, regulatory requirements, and legal orders, or for use to prepare for or defend against product liability, breach of contract, consumer protection, or warranty claims; (c) to perform diagnostics and prognostics of components of the Vehicle; (d)

to conduct research or efforts to improve, repair, enhance safety of, or develop products, services, or technology, provided, however, that (1) only Deidentified Covered Driver Data is disclosed to Third Parties to fulfill this purpose; and (2) marketing is excluded from this purpose; and (e) to conduct investigations of potential product quality or safety issues; to determine or effectuate Vehicle field actions, including customer satisfaction campaigns, technical service bulletins, compliance recalls, and safety recalls; to detect or respond to cybersecurity incidents; or to administer and fulfill Vehicle warranties; and

- b. Provide a written statement to the Washington State Attorney General confirming that all such information has been Deleted or destroyed.

64. Notwithstanding the requirements set forth in Paragraph 63, Defendants may, within ninety (90) days of the Effective Date, send an email to Consumers whose Covered Driver Data was collected and retained prior to January 16, 2025 to request the Consumer's Affirmative Express Consent to maintain that data. Defendants must Delete such prior-retained Covered Driver Data where (1) a Consumer does not provide their Affirmative Express Consent; (2) the Consumer does not respond to the request within thirty (30) days after the request is made; or (3) the data has not been Deidentified.

65. Copy of Covered Driver Data: Defendants must provide an easily accessible method by which a Consumer may request a copy of their Covered Driver Data and a list of the categories of Third Parties with whom Defendants shared any Covered Driver Data. The method chosen must: (1) consider the ways in which Consumers normally interact with Defendants; (2) enable the Consumer to submit the request to the Defendants at any time; (3) be described through a Clear and Conspicuous disclosure; and (4) be easy for Consumers to execute, requiring a minimal number of steps. Upon request by a Consumer to obtain a copy of their Covered Driver Data, Defendants must provide confirmation of receipt of the Consumer's request and must timely (within forty-five (45) days after receipt of the request) process all such requests. Defendants may require a Consumer to provide Defendants with information necessary to complete such request but must not use, provide access to, or disclose any information collected for the request for any other purpose. Nothing in this Paragraph shall abrogate Defendants' rights to: (i) avail itself of any and all rights, exceptions, and exemptions existing under any state or federal law, or (ii) retain a subset of a Consumer's Covered Driver Data to comply with its legal, regulatory, or other obligations. Defendants are not obligated to comply with the requirements under this Paragraph when the requirements conflict with Defendants' ability to comply with federal, state, or local laws or regulations; any civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by

federal, state, local, or other governmental authorities; or any transactional, tax, escheatment, corporate accountability, or other legitimate business needs compatible with the context in which the Consumer provided the information. The obligations set forth in this Paragraph shall continue until January 13, 2046.

66. Notice of Consumer Options: Within (30) days of the expiration of the litigation hold on Covered Driver Data (the “Lit Hold Expiration Date”), Defendants must post Clearly and Conspicuously on their public-facing website(s), a notice that Consumers may request deletion of their Covered Driver Data and a copy of their Covered Driver Data with a link to Defendants’ online Consumer Privacy Request Form, in accordance with this Judgment (“Notice”). Defendants must leave this Notice in place for six (6) months after posting it. Within thirty (30) days of the Lit Hold Expiration Date, Defendants must also email the Notice to Consumers that were enrolled in OnStar at any time between January 1, 2018 through the Effective Date.

67. Consumer Complaints: Defendants must maintain a point of contact, such as a dedicated e-mail address, for the Plaintiff or any U.S. federal or state governmental agency charged with enforcement of a U.S. federal or state Consumer Protection Law or Personal Information Protection Law (“Consumer Protection Agency”) for the receipt of User complaints relating to Covered Driver Data or the disclosure of Personal Information. Defendants must promptly review and respond

to all User complaints submitted by a Consumer Protection Agency.

68. Retention Schedule – Internal: Within one hundred and eighty (180) days of the Effective Date, Defendants must document and adhere to a retention schedule for Covered Driver Data, setting forth: (1) the purpose(s) for which each type of Covered Driver Data is collected; (2) the specific business needs for retaining each type of Covered Driver Data; and (3) the specific timeframe for deleting each type of Covered Driver Data (absent any intervening deletion requests from consumers), limited to the shortest time necessary to fulfill the purpose for which the data was collected, or as otherwise consistent with Paragraph 42.b. The obligations set forth in this Paragraph shall continue until January 13, 2046.

69. Retention Schedule – Public: Within one hundred and eighty (180) days of the Effective Date, Defendants must document, adhere to, and make publicly available from a link on the Defendants' Apps or the home page of their website(s), a retention schedule for Covered Driver Data setting forth: (1) the purpose for collecting and retaining each type of Covered Driver Data, and (2) the specific timeframe set for deleting each type of Covered Driver Data. The obligations set forth in this Paragraph shall continue until January 13, 2046.

70. Retention Schedule – Updates: Prior to collecting or using any new type of Covered Driver Data that was not being collected as of the date of creation of retention schedules required by Paragraphs 68 and 69, Defendants must update those

retention schedules.

IV. DOCUMENT RETENTION

71. After the Effective Date, Defendants must maintain the following records for a period of not less than five (5) years:

- a. Accounting records showing the revenues from all OnStar goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- b. Personnel records showing, for each employee providing OnStar services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination if the termination is related to non-compliance with this Judgment;
- c. Copies of all Consumer complaints that relate to Covered Driver Data and disclosure of Personal Information, whether received directly or indirectly, including from a Consumer Protection Agency pursuant to Paragraph 67, and any written response;
- d. A copy of each widely disseminated representation by Defendants, including a copy of each Privacy Notice, that describes the extent to which Defendants maintain or protect the privacy of any Covered Driver Data, including any representation concerning a material change

in any website or other service controlled by Defendants that relates to the privacy of Covered Driver Data.

- e. Reports, assessments, and documentation required by this Judgment in Paragraphs 32, 33.d, 33.e, 36, 39, 50, 51, 53, 54, 57, 58, and 60;
- f. Records showing Affirmative Express Consent for any individual Consumer on which Defendants have relied to collect, use, or disclose Covered Driver Data, including the specific notice(s) that individual Consumers viewed and consented to, and the time and date of consent;
- g. Records of all Consumer requests processed pursuant to Paragraphs 62 and 65;
- h. Copies of all subpoenas and subpoena responses with law enforcement agencies located in the U.S. if such subpoenas relate to Defendants' compliance with this Judgment; and
- i. All materials the Third-Party Assessor relied upon to conduct the Third-Party Privacy Assessments to the extent identified by the Third-Party Assessor in the Third-Party Assessment Report.

V. MONETARY PAYMENT

72. No later than thirty (30) days after the Effective Date, Defendants shall pay the sum of Two Hundred and Twenty Million Dollars (\$220,000,000.00) to be

divided by and among the participating states² and paid by Defendants directly to the Plaintiff in the amount designated in Paragraph 73.

73. Defendants must pay \$4,726,779 to Delaware. Payment shall be made by wire pursuant to instructions previously provided by the Delaware Attorney General for the Consumer Protection Unit (“CPU”). CPU shall place all funds received for CPU in the State of Delaware’s Consumer Protection Fund, and such funds may be utilized for any lawful purpose.

VI. RELEASE

74. Following full payment of the amounts due under this Judgment, the Plaintiff shall release and discharge Defendants from all civil claims that the Plaintiff could have brought under the Consumer Protection Law and Consumer Privacy Law based on Defendants’ conduct as set forth in the Complaint up to and including the Effective Date. Nothing contained in this paragraph shall be construed to limit the ability of the Plaintiff to enforce the obligations that Defendants have under this Judgment. Further, nothing in this Judgment shall be construed to (a) create, waive, or limit any private right of action; or (b) excuse or exempt Defendants from complying with any state or federal law, rule, or regulation in the future.

75. Notwithstanding any term of this Judgment, any and all of the following forms of liability are specifically excluded from the release in Paragraph 74 above

² *Supra*, note 1.

as to any entity or person, including Defendants:

- a. Any criminal liability that any person or entity, including Defendants, have or may have to the States; and
- b. Any civil liability or administrative liability that any person or entity, including Defendants, have or may have to the States under any statute, regulation, or rule not expressly covered by the release in Paragraph 74 above, including but not limited to, any and all of the following claims: (i) State or federal antitrust violations; (ii) State or federal securities violations; or (iii) State or federal tax claims.

VII. NO ADMISSION OF LIABILITY

76. In stipulating to the entry of this Judgment, Defendants do not admit to any violation or liability arising from any state, federal, or local law.

77. Nothing contained in this Judgment shall be construed as an admission or concession of liability by Defendants, nor to any express or implied allegations relating to current or historical data processing policies or practices. By entering into this Judgment, Defendants do not intend to create any legal or voluntary standard of care and expressly deny that any practices, policies, or procedures inconsistent with those set forth in this Judgment violate any applicable legal standard. This Judgment is not intended to be and shall not be construed as, deemed to be, represented as, or relied upon in any manner by any party in any civil, criminal, or administrative

proceeding before any court, administrative agency, arbitration, or other tribunal as an admission, concession, or evidence that Defendants have violated any federal, state, or local law, or that Defendants' current or prior practices related to their Privacy Program is or was not in accordance with any federal, state, or local law.

VIII. GENERAL PROVISIONS

78. Nothing in this Judgment may be construed to limit the authority or ability of the Plaintiff to protect the interests of Delaware or the people of Delaware. This Judgment shall not bar the Plaintiff or any other governmental entity from enforcing laws, regulations, or rules against Defendants for conduct subsequent to or otherwise not covered by this Judgment.

79. Nothing in this Judgment may be construed as excusing or exempting Defendants from complying with any state, federal, or other jurisdiction's law, rule, or regulation, nor shall any provision of this Judgment be construed in a manner to prevent Defendants from complying with any such law, regulation, or rule where in conflict with this Judgment. Furthermore, no provisions of this Judgment shall be construed as authorizing, permitting, or requiring Defendants to engage in any acts or practices prohibited by any state, federal, or other jurisdiction's law, rule, or regulation.

80. Defendants must not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices that are prohibited by

this Judgment or that would circumvent any term of this Judgment. Defendants must not knowingly cause, permit, or encourage any other persons or entities acting on their behalf, to engage in practices prohibited by this Judgment.

81. Defendants must pay all court costs associated with the filing of this Judgment, as applicable.

82. Plaintiff and Defendants agree to waive any attorneys' fees as a prevailing party under any statute, regulation, or rule.

83. This Judgment may not be construed to waive any claims of sovereign immunity that Delaware may have in any action or proceeding.

84. Defendants must deliver a copy of this Judgment to, and otherwise fully apprise, its Chief Executive Officer, General Counsel, Chief Privacy Officer, and Board of Directors within ninety (90) days of the Effective Date. To the extent Defendants replace any of the above-listed officers or directors, Defendants must deliver a copy of this Judgment to their replacements within ninety (90) days from the date on which such person assumes his or her position with Defendants unless such person has previously been provided a copy pursuant to this Judgment.

85. If any portion of this Judgment is held invalid or unenforceable, the remaining terms of this Judgment will not be affected and will remain in full force and effect.

86. Solely for the purposes of entry of this Judgment, Defendants waive

any defect associated with service of the Plaintiff's Complaint and does not require issuance or service of process of a summons. Further, Defendants waive any statutorily required notice associated with the commencement of this action, including any requirement to seek injunctive relief.

87. The Court retains jurisdiction over this Judgment and the Parties hereto for the purpose of enabling any party to the Judgment to apply to the Court at any time for such further orders and directions as may be necessary or appropriate for the construction or the carrying out of this Judgment, enforcing or modifying this Judgment, and for the purpose of granting such additional relief as may be necessary and appropriate.

88. The Parties hereby acknowledge that their undersigned representative or representatives are authorized to enter into and execute this Judgment. Defendants are and have been represented by legal counsel and have been advised by their legal counsel of the meaning and legal effect of this Judgment.

89. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which will be considered one and the same Judgment.

IX. NOTICES

90. Any notices or other documents required to be sent to the Parties

pursuant to the Judgment shall be sent by electronic mail. Nothing herein prohibits the sending party from simultaneously providing notice by electronic mail and by United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. Any notices or other documents sent pursuant to the Judgment shall be sent to:

For Plaintiff:

John Allen Eakins
Deputy Attorney General
Delaware Department of Justice
820 N. French Street, 5th Floor
Wilmington, Delaware 19801
John.eakins@delaware.gov

Alternative Point of Contact:

Brian Canfield
Deputy Attorney General
Delaware Department of Justice
820 N. French Street, 5th Floor
Wilmington, Delaware 19801
Brian.canfield@delaware.gov

For Defendants:

Christina Montgomery
Chief Privacy and Trust Officer & Assistant General Counsel
1240 Woodward Ave, Detroit, MI 48265
Mail Code 482-22381-1101
Email: christina.montgomery@gm.com

Phyllis Sumner
Elizabeth Adler
1180 Peachtree Street, NE, Suite 1600 Atlanta, GA 30309

Email: PSumner@kslaw.com
Email: EAdler@kslaw.com

A Party may update its designee or address by sending written notice to the other Party informing them of the change.

X. MEET AND CONFER

91. If Plaintiff has reason to believe that Defendants have failed to comply with this Judgment, and if in the Plaintiff's sole discretion the failure to comply does not threaten the health or safety of citizens and/or does not create an emergency requiring immediate action, the Plaintiff shall notify Defendants of such failure to comply and Defendants shall have thirty (30) days from receipt of such notice to provide a good faith written response, including either a statement that Defendants believe they are in full compliance or otherwise a statement explaining how the violation occurred, how it has been addressed or when it will be addressed, and what Defendants will do to make sure the violation does not happen again. The Plaintiff may agree to provide Defendants more than thirty (30) days to respond.

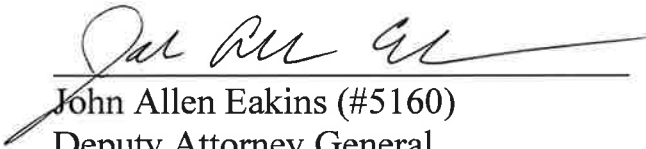
92. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Judgment, or to compromise the authority of the Plaintiff to initiate a proceeding for any failure to comply with this Judgment after receiving the response from Defendants described in Paragraph 91 above, the Plaintiff determines that an enforcement action is in the public interest.

The Undersigned Parties enter into this Consent Judgment in the matter of *State of Delaware, ex rel. Kathleen Jennings, Attorney General of the State of Delaware v. GENERAL MOTORS LLC, GENERAL MOTORS HOLDINGS LLC, and ONSTAR, LLC*:

Dated: October 29, 2026

FOR PLAINTIFF:

**DEPARTMENT OF JUSTICE
STATE OF DELAWARE**


John Allen Eakins (#5160)

Deputy Attorney General

Brian Canfield (#7027)

Deputy Attorney General

820 N. French Street, 5th Floor

Wilmington, DE 19801

(302) 577-8400

Attorneys for the Plaintiff

Date: October 29, 2026

FOR DEFENDANTS:

Date: Oct. 29, 2026

By 

Phyllis B. Sumner,
Elizabeth Adler,
King & Spading LLP
1180 Peachtree Street NE
Atlanta, GA 30309
Phone: (404) 572-4799
PSumner@KSLAW.com
Eadler@KSLAW.com

Counsel for General Motors LLC; General Motors Holdings LLC; and OnStar, LLC