UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

LORIA SPADAFORE and THOMAS SPADAFORE individually and on behalf of all others similarly situated, Plaintiff, v. FCA US LLC, d/b/a STELLANTIS NORTH AMERICA, Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Loria Spadafore and Thomas Spadafore ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through undersigned counsel, bring this Class Action Complaint against Defendant FCA US LLC, d/b/a Stellantis North America ("FCA" or "Defendant") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. This class action arises from Defendant's failure to implement and maintain reasonable data security procedures and practices, resulting in a data breach in or around December 25, 2025 (the "Data Breach") in which unauthorized third parties accessed and/or exfiltrated Plaintiffs' and Class Members' highly sensitive

personal information and contact information, including but not limited to: names, phone numbers, addresses, dates of birth, Social Security numbers, and other personal information defined as "Personally Identifiable Information" ("PII") under applicable federal and state law.

2. Defendant FCA US LLC is a limited liability company headquartered in Auburn Hills, Michigan, operating brands including Chrysler, Dodge, Jeep, and Ram.

3. Defendant's failure to secure Chrysler's servers and databases jeopardized the security of Plaintiffs' and Class Members' Personal Information, and exposed Plaintiffs and Class Members to fraud and identity theft.

4. Defendant's conduct led to the Data Breach. Hackers exfiltrated Plaintiffs and Class Members' data, invaded Plaintiffs and Class Members' privacy, and exposed Plaintiffs and Class Members to identity theft and fraud. Accordingly, these Plaintiffs and Class Members now must take action to protect themselves from identity theft and fraud.

PARTIES

Plaintiffs

5. Plaintiff Loria Spadafore is a resident of DuPage County, Illinois who purchased a 2023 Jeep Gladiator with her husband, Thomas Spadafore. The purchase

required Ms. Spadafore to submit PII to FCA US LLC, including her name, address, date of birth, phone number, Social Security number, and other personal information.

6. Plaintiff Thomas Spadafore is a resident of DuPage County, Illinois who purchased a 2023 Jeep Gladiator with his wife, Loria Spadafore. The purchase required Mr. Spadafore to submit PII to FCA US LLC, including his name, address, date of birth, phone number, Social Security number, and other personal information.

Defendant

7. Defendant FCA US LLC is a limited liability company that designs, manufactures, sells, and leases vehicles. It operates automaker brands including Chrysler, Dodge, Jeep, and Ram. FCA US, LLC's Corporate Headquarters are located at 1000 Chrysler Drive, Auburn Hills, Michigan 48326. FCA US LLC is a subsidiary of the corporation Stellantis N.V.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class Members, the action is a class action in which one or more Class Members are citizens of states different from Defendant.

9. The Court has personal jurisdiction over Defendant because Defendant is headquartered in Michigan, maintains its principal place of business in Michigan, and conducts substantial business in Michigan.

10. Venue properly lies in this judicial district because Defendant is headquartered in Auburn Hills, Michigan.

FACTUAL ALLEGATIONS

Defendant Collects and Stores Personal Information

11. Defendant FCA operates the automaker Chrysler, which manufactures and sells vehicles.

12. In the regular course of business, Defendant routinely collects, stores, and maintains highly sensitive personal information, including personally identifiable information ("PII") from individuals that purchase Chrysler vehicles.

13. Defendant benefits from collecting the PII of its customers, including Plaintiffs and Class Members. Defendant collects PII in part to conduct sales, perform research and analytics, to personalize content for customers, to advertise and market to customers, to support its business operations, and to conduct business transactions.[1]

[1] *See* FCA, *FCA US Privacy Policy*, https://www.chrysler.com/crossbrand_us/privacy (last accessed Jan. 7, 2026).

The Data Breach

14. On or around December 25, 2025, the ransomware group Everest breached Defendant's systems due to Defendant's failure to secure its databases, gaining access to 1 terabyte of Plaintiffs' and Class Members' sensitive Personal Information.[2]

15. Everest threatened to publish Plaintiffs' and Class Members' Personal Information unless a ransom was paid.[3]

16. On information and belief, Defendant refused to pay the ransom demanded by Everest and Everest published Personal Information belonging to Plaintiffs and Class Members on January 4, 2026.

17. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

18. Defendant failed to secure its databases consistent with industry standards and best practices, allowing Everest to exfiltrate PII.

[2] *See* SC Media, *Chrysler allegedly compromised by Everest ransomware gang*, https://www.scworld.com/brief/chrysler-allegedly-compromised-by-everest-ransomware-gang (last accessed Jan. 7, 2026).
[3] *See id*.

19. Upon information and belief, the ransomware group Everest and other cybercriminals have obtained *inter* alia, names, addresses, dates of birth, Social Security numbers, and other highly sensitive PII following the Data Breach.

Defendant Knew That Criminals Target PII

20. At all relevant times, Defendant knew, or should have known that Plaintiffs' and Class Members' PII was a target for malicious actors. In September, unauthorized third parties infiltrated the databases of FCA's parent company Stellantis, gaining access to customer information.[4]

21. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' PII from cyber-attacks that Defendant should have anticipated and guarded against.

22. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as Social Security numbers ("SSNs")—is valuable and frequently targeted by criminals. Indeed, "[d]ata

[4] *See* Stellantis, *Third-Party Platform Data Incident*, https://media.stellantisnorthamerica.com/newsrelease.do?id=27079&mid=1#:~:text=Stellantis's%20response%20to%20the%20incident%20includes:%20*,wish%20to%20verify%20communications%20should%20contact%20Stellantis (last accessed Jan. 8, 2026).

breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[5]

23. PII is a valuable property right.[6] The value of PII as a commodity is measurable.[7] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[8] American companies spend many billions of dollars on acquiring personal data of consumers.[9] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[5] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[6] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[7] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[8] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD LIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last accessed Oct. 5, 2023).

[9] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last accessed Oct. 5, 2023) (estimated to have spent over $19 billion in 2018).

24. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

25. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

26. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

27. Theft of PII is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII to exhaust financial accounts, receive medical

[10] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

treatment, start new utility accounts, and incur charges and credit in a person's name.[11]

28. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[13]

---

[11] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 5, 2023).

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[13] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

29. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits, or; filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[14]

30. Identity theft is a very difficult problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[15]

31. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new SSN, a breach

[14] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Oct. 5, 2023).

[15] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Oct. 5, 2023).

victim has to demonstrate ongoing harm from misuse of his SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

32. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[16]

33. For these reasons, the information compromised in the Data Breach is significantly more valuable than the loss of basic financial information, because there, victims can cancel or close credit or debit card accounts. Upon information and belief, the information compromised by the Data Breach—for example, a Social Security number—is exceedingly difficult, if not impossible, to change.

34. It is within this context that Plaintiffs and Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

---

[16] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

Defendant Fail to Comply With Industry Standards

35. Cyber security experts routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the information which they collect and maintain.

36. As a result, several best practices have been identified that, at a minimum, should be implemented by entities in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

37. Defendant failed to follow, enforce, or maintain the aforementioned best practices. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Damages Sustained by Plaintiffs and the Other Class Members

38. Plaintiffs and Class Members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

39. Plaintiffs and Class Members had a reasonable expectation of privacy in their sensitive PII while purchasing their vehicle. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would fail to protect their PII. Indeed, Plaintiffs and Class Members purchased Defendant's vehicle with the reasonable expectation that Defendant would keep their PII secure and inaccessible to unauthorized parties. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII from criminal theft and misuse.

40. Plaintiffs and all other Class Members have suffered injury and

damages, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

41. As a result of Defendant's failures, Plaintiffs and Class Members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII. Indeed, Plaintiffs' damages are not merely speculative. Consequently, Plaintiffs and Class Members now face a substantially increased risk of identity that is plausibly imminent, considering the actual instances of fraud already suffered by other Class Members.

CLASS ALLEGATIONS

42. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

43. Plaintiffs bring this action on behalf of themselves and all Members of the following Classes of similarly situated persons:

> **Nationwide Class**
> All persons in the United States whose PII was accessed by and disclosed to unauthorized persons as a result of the Data Breach.

Illinois Subclass
All persons in the state of Illinois whose PII was accessed by and disclosed to unauthorized persons as a result of the Data Breach.

44. The Nationwide Class and Illinois Subclass are collectively referred to herein as the "Class."

45. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

46. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

47. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

48. While the precise number of Class Members has not yet been determined, the Members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Upon information and belief, the Data Breach affected tens of thousands of individuals who are geographically dispersed.

49. Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

c. Whether an implied contract existed between Class Members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

d. Whether Defendant breached its duties to protect Plaintiffs' and Class Members' PII; and

e. Whether Plaintiffs and Class Members are entitled to damages and the measure of such damages and relief.

50. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

51. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed Members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore

arise from the same practices or course of conduct that give rise to the claims of all Class Members.

52. Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are adequate representatives of the Class in that Plaintiffs have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

53. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class)

54. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

55. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

56. Defendant knew the risks of collecting and storing Plaintiffs' and Class Members' PII and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted businesses that collect sensitive PII in recent years.

57. Given the nature of Defendant's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

58. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and

software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class Members' PII.

59. It was reasonably foreseeable to Defendant that failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII to unauthorized individuals.

60. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

61. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

62. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable

given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

63. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' PII to unauthorized individuals.

64. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care, and its negligence and negligence per se, that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure, publication, and theft of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) the continued risk to their PII which remains in Defendant's possession; and (vi) lost

time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that they face and will continue to face. In addition, Class Members already have suffered actual fraud and identity theft as alleged herein, demonstrating how imminent the threat of such fraudulent activity and damages are to all Class Members.

COUNT II
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Nationwide Class)

65. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

66. Plaintiffs and Class Members provided Defendant their PII in confidence, believing that Defendant would protect that information. Plaintiffs and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class Members' PII created a fiduciary relationship between Defendant, on the one hand, and Plaintiffs and Class Members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class Members' PII.

67. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. Defendant

breached that duty by failing to properly protect the integrity of its systems containing Plaintiffs' and Class Members' PII and failing to safeguard Plaintiffs' and Class Members' PII that they collected.

68. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach. In addition, upon information and belief, Class Members already have suffered actual fraud and identity theft, demonstrating how imminent the threat of such fraudulent activity and damages are to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

69. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

70. In connection with purchasing Defendant's vehicle, Plaintiffs and Class Members entered into implied contracts with Defendant.

71. Pursuant to these implied contracts, Plaintiffs and Class Members provided Defendant with their PII. In exchange, Defendant agreed to, among other things, and Plaintiffs understood that Defendant would: (1) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' PII; and (2) protect Plaintiffs' and Class Members' PII in compliance with federal and state laws and regulations and industry standards.

72. The protection of PII was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand. Had Plaintiffs and Class Members known that Defendant would not adequately protect its customer's PII, they would not have purchased Defendant's vehicles.

73. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Defendant with their PII and paid for Defendant's vehicles.

74. Defendant breached its obligations under its implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members'

PII in a manner that complies with applicable laws, regulations, and industry standards.

75. Defendant's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and Class Members have suffered from the Data Breach.

76. Plaintiffs and Class Members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or through its insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

77. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

78. This claim is pleaded in the alternative to the breach of implied contract claim.

79. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of monies paid for Defendant's vehicles.

80. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefitted from the receipt of Plaintiffs' and Class Members' PII, as this information was used for Defendant's benefit, including facilitating payment in purchasing Defendant's vehicles, conducting research and analytics, supporting Defendant's business operations, and marketing.

81. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

82. Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

83. Defendant should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by them as a result of its conduct and Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("ICFA")
815 ILCS 505/2, et seq.
(On behalf of Plaintiffs and the Illinois Subclass)

84. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

85. Defendant manufactured and sold vehicles in the State of Illinois.

86. Plaintiffs and Class Members purchased their vehicles and other related services from Defendant for personal, family, or household purposes.

87. Defendant engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class Members' Personal Information in a manner that complied with applicable laws, regulations, and industry standards.

88. Defendant makes explicit statements to Plaintiffs and Class Members that their Personal Information will remain private.

89. Defendant further violated the ICFA by failing to notify Plaintiffs and Class Members of the Data Breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify

Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. *See* 815 ILCS 530/20.

90. Due to the Data Breach, Plaintiffs and Class Members have lost property in the form of: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Personal Information which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other Members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 21, 2026

/s/ E. Powell Miller
E. Powell Miller (P39487)
Gregory A. Mitchell (P68723)

THE MILLER LAW FIRM, P.C.
950 W. University Dr., Ste. 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
gam@millerlawpc.com

Bradley K. King
AHDOOT & WOLFSON, PC
521 Fifth Avenue, 17th Floor
New York, New York 10175
Telephone: (917) 336-0171
Facsimile: (917) 336-0177
bking@ahdootwolfson.com

Attorneys for Plaintiffs and the Proposed Class